

特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局(43) 国際公開日  
2004年11月4日 (04.11.2004)

PCT

(10) 国際公開番号  
WO 2004/095301 A1

(51) 国際特許分類7: G06F 15/00, H04L 9/32

(MIURA, Takayuki) [JP/JP]. 勝部 友浩 (KATSUBE, Tomohiro) [JP/JP]. 鈴木 直志 (SUZUKI, Naoshi) [JP/JP].

(21) 国際出願番号: PCT/JP2004/005740

(22) 国際出願日: 2004年4月21日 (21.04.2004)

(25) 国際出願の言語: 日本語

(74) 代理人: 中村 友之 (NAKAMURA, Tomoyuki); 〒1050001 東京都港区虎ノ門1丁目2番3号虎ノ門第一ビル9階三好内外国特許事務所内 Tokyo (JP).

(26) 国際公開の言語: 日本語

(30) 優先権データ:  
特願2003-115754 2003年4月21日 (21.04.2003) JP  
特願2004-095272 2004年3月29日 (29.03.2004) JP(71) 出願人 (米国を除く全ての指定国について): ソニー  
株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001  
東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および

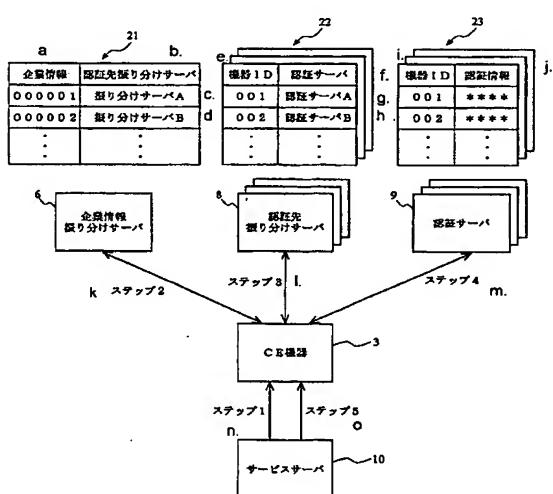
(75) 発明者/出願人 (米国についてのみ): 三浦 貴之

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

/統葉有/

(54) Title: TERMINAL DEVICE AUTHENTICATION SYSTEM

(54) 発明の名称: 端末機器認証システム



- a...CORPORATE INFORMATION
- b...AUTHENTICATION DESTINATION DISTRIBUTING SERVER
- c...DISTRIBUTING SERVER A
- d...DISTRIBUTING SERVER B
- e...DEVICE ID
- f...AUTHENTICATING SERVER
- g...AUTHENTICATING SERVER A
- h...AUTHENTICATING SERVER B
- i...DEVICE ID
- j...AUTHENTICATION INFORMATION
- 6...CORPORATE INFORMATION DISTRIBUTING SERVER
- 8...AUTHENTICATION DESTINATION DISTRIBUTING SERVER
- 9...AUTHENTICATING SERVER
- 3...CE DEVICE
- 10...SERVICE SERVER
- k...STEP 2

(57) Abstract: A device authentication system capable of appropriately distributing authentication destinations of CE devices. The device ID of a CE device (3) includes corporate information. The CE device (3) uses the corporate information to send, to a corporate information distributing server (6), an inquiry about an authentication destination distributing server (8) for connection, and further uses the device ID to send, to the authentication destination distributing server (8), an inquiry about an authenticating server (9) for connection. Then, the CE device (3) receives an authentication from the authenticating server (9) and transmits the authentication result to a service server (10).

(57) 要約: C E 機器の認証先を適切に振り分けることのできる機器認証システムである。C E 機器 (3) の機器 ID は、企業情報を含んでいる。C E 機器 (3) は、企業情報を用いて企業情報振り分けサーバ (6) に接続先の認証先振り分けサーバ (8) を問い合わせ、更に、機器 ID を用いて認証先振り分けサーバ (8) に接続先の認証サーバ (9) を問い合わせる。そして、C E 機器 (3) は、認証サーバ (9) で認証を受け、認証結果をサービスサーバ (10) に送信する。



(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:  
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイドスノート」を参照。

## 明細書

## 端末機器認証システム

## 10 技術分野

本発明は、機器認証システムなどに関し、特に、機器を認証する認証サーバが複数存在する場合に、機器 ID と認証する認証サーバを予め対応付けておくことにより、適切な認証サーバで認証を行うものに関する。

## 15 背景技術

近年、CE (C E : C on s u m e r E l e c t r o n i c s) 機器が普及しつつある。CE 機器とは、例えば、ビデオデッキ、ハードディスクレコーダ、ステレオ、テレビなどのオーディオビジュアル機器や、パーソナルコンピュータ、デジカメ、カムコーダ、P D A (P e r s o n a l D i g i t a l A s s i s t a n c e) 、ゲーム機、ホームルータ等の電子機器や、炊飯器、冷蔵庫などの家電製品や、その他の電子機器にコンピュータを内蔵させ、ネットワークを介したサービスを利用できるものである。

そして、CE 機器からサーバにアクセスしてコンテンツをダウンロードするなどし、ユーザはサーバが提供するサービスを利用できる。

サーバが提供するサービスには、CE機器全般に提供するものと、機器認証された特定のCE機器に提供するものがある。

サーバは、機器認証を要するサービスを提供する場合、そのCE機器を認証サーバで認証し、認証された場合にサービスを提供する。

5 第8図は、CE機器の認証システム100の構成の一例を示した図である。

この認証システムは、未公開の特許文献（特願2002-144896）で提案されているものである。

従来は、CE機器の認証の際、認証情報（パスフレーズ、機器IDなどのセキュリティ上重要な情報）を直接サービスサーバに送信していたが、サービスサーバは、個人や任意の団体が運営するが多く、セキュリティ上問題があるため、この認証システムでは機器認証を代行する機器認証サーバを別途設けたものである。

10 認証システム100では、CE機器101、認証サーバ102、サービスサーバ103がインターネット104で接続可能に配設されている。

ユーザは、CE機器101をサービスサーバ103に接続してサービスサーバ103が提供するサービスを利用することができる。

ユーザが、機器認証を要するサービスの提供を希望した場合、サービスサーバ103は、CE機器101に認証サーバ102の情報を送信して認証サーバ102で機器認証するようにCE機器101に要求し、これに応じてCE機器101は認証サーバ102で機器認証を受ける。

サービスサーバ103は、CE機器101が認証サーバ102で機器認証を受けたことを確認し、CE機器101にサービスを提供する。

この認証システムでは、CE機器101の認証を行う際、認証サーバ102が单一であったため、サービスサーバ103は認証を要求するC

E機器101がどの認証サーバで認証されるか（第8図の場合認証サーバ102）を把握することができた。

従って、サービスサーバ103は、機器認証を要求する際に、CE機器101へ認証サーバ102の情報を渡すことが可能であった。

5 しかし、認証サーバ102が複数存在する場合、アクセスしたCE機器101に対し、サービスサーバ103はCE機器101に適当な認証サーバ102の情報を送信するためのスキームが用意されていない。従って、CE機器101は適切な認証サーバ102の情報を取得することができないという問題があった。

10 CE機器101を製造販売する事業者は複数存在するなどの理由により、複数の認証サーバ102を用意し、アクセスしてきたCE機器101によって認証サーバ102を振り分ける仕組みが必要とされている。

また、CE機器の機器認証に関する技術ではないが、認証サーバが複数存在し、アクセスしてきたユーザに応じて認証サーバを振り分けるものとして以下の発明がある。

特開2002-197061号公報記載の技術は、ISP（Internet Service Provider）に登録しているユーザが、一般ユーザであるか特定ユーザであるかに基づいてユーザの認証処理を振り分けるものである。振り分けの手順は以下の通りである。

20 まず、一般ユーザ用電話番号と特定ユーザ用電話番号が振り分けられている。そして、振り分けサーバでは電話番号に基づいて一般／特定を決定して、それぞれの認証サーバへ振り分ける。更に、端末からユーザID／パスワードが振り分けサーバへ送信される。

特開2000-331095号公報記載の技術は、ユーザからのアクセスを受けた際に、ユーザ登録時にIDを発行した認証サーバにユーザのアクセスの振り分けを行わせるものである。

振り分けの手順は以下の通りである。

まず、ユーザは、ユーザ ID とパスワードを振り分けサーバに送信する。そして、振り分けサーバは、ユーザ ID の所定の桁からユーザ ID を発行した認証サーバを判別する。更に、判別した認証サーバにユーザ

5 ID とパスワードを送信し、ユーザを認証する。

ところで、一般的な事業形態として、CE 機器の認証先を事業者別に振り分けた後に、事業者が更に複数の認証サーバを用意していることが考えられる。上記の特許文献の技術を利用したとしても、このような場合に対応することは困難である。

10 そこで、本発明の目的は、CE 機器の認証先を適切に振り分けることのできる機器認証システムなどを提供することである。

## 発明の開示

本発明は、前記目的を達成するために、端末機器に機器認証を要する  
15 サービスを提供する場合に、前記端末機器に第 1 の振り分けサーバへの接続情報を送信し、前記端末機器から認証結果を受信するサービスサーバと、端末機器から第 1 の振り分け情報を受信し、当該第 1 の振り分け情報に対応する第 2 の振り分けサーバへの接続情報を送信する第 1 の振り分けサーバと、端末機器から第 2 の振り分け情報を受信し、当該第 2  
20 の振り分け情報に対応する認証サーバへの接続情報を送信する第 2 の振り分けサーバと、端末機器から認証情報を受信して機器認証し、認証結果を前記端末機器に送信する認証サーバと、から構成されたことを特徴とする端末機器認証システムを提供する（第 1 の構成）。

また、本発明は、第 1 の構成の端末機器認証システムでサービスサー  
25 バが提供するサービスを利用する端末機器が、前記サービスサーバから、第 1 の振り分けサーバへの接続情報を受信する第 1 の受信手段と、前記

第1の振り分けサーバに、前記第1の受信手段で受信した接続情報を用いて接続して第1の振り分け情報を送信する第1の送信手段と、前記第1の振り分けサーバから、前記送信した第1の振り分け情報に対応した第2の振り分けサーバへの接続情報を受信する第2の受信手段と、前記第2の振り分けサーバに、前記第2の受信手段で受信した接続情報を用いて接続して第2の振り分け情報を送信する第2の送信手段と、前記第2の振り分けサーバから、前記送信した第2の振り分け情報に対応した認証サーバへの接続情報を受信する第3の受信手段と、前記認証サーバに、前記第3の受信手段で受信した接続情報を用いて接続して認証情報を送信する認証情報送信手段と、前記認証情報送信手段で送信した認証情報による認証結果を前記認証サーバから受信する認証結果受信手段と、前記認証結果受信手段で受信した認証結果を前記サービスサーバに送信する認証結果送信手段と、を具備するように構成することができる（第2の構成）。

また、本発明は、第1の構成の端末機器認証システムで端末機器に第2の振り分けサーバへの接続情報を提供する第1の振り分けサーバが、端末機器からの接続を受け付け、前記端末機器から第1の振り分け情報を受信する受信手段と、前記受信した第1の振り分け情報に対応する第2の振り分けサーバへの接続情報を前記端末機器に送信する送信手段と、を具備するように構成することができる（第3の構成）。

また、本発明は、端末機器に機器認証を要するサービスを提供する場合に、前記端末機器から振り分け情報を受信し、前記受信した振り分け情報を用いて振り分けシステムから認証サーバへの接続情報を受信し、前記受信した接続情報を前記端末機器に送信し、前記認証サーバでの認証結果を前記端末機器から受信するサービスサーバと、前記サービスサーバから前記振り分け情報を受信し、前記受信した振り分け情報に対応

する認証サーバへの接続情報を前記サービスサーバに送信する前記振り分けシステムと、前記端末機器から認証情報を受信して前記端末機器の機器認証を行い、前記機器認証の認証結果を前記端末機器に送信する前記認証サーバと、から構成されたことを特徴とする端末機器認証システムを提供することができる（第4の構成）。

また、本発明は、第4の構成の端末機器認証システムでサービスサーバに認証サーバへの接続情報を提供する振り分けシステムが、サービスサーバから振り分け情報を受信する振り分け情報受信手段と、前記受信した振り分け情報に対応する認証サーバへの接続情報を送信する接続情報送信手段と、を具備するように構成することができる（第5の構成）。

また、本発明は、第4の構成の端末機器認証システムで端末機器にサービスを提供するサービスサーバが、端末機器から振り分け情報を受信する振り分け情報受信手段と、前記受信した振り分け情報を振り分けシステムに送信する振り分け情報送信手段と、前記送信した振り分け情報に対応する認証サーバへの接続情報を前記振り分けシステムから受信する接続情報受信手段と、前記受信した接続情報を前記端末機器に送信する接続情報送信手段と、を具備するように構成することができる（第6の構成）。

また、本発明は、第5の構成の振り分けシステムにおいて、前記振り分け情報は、第1の振り分け情報と、第2の振り分け情報から構成され、前記振り分けシステムは、サービスサーバから前記第1の振り分け情報を受信し、当該第1の振り分け情報に対応する第2の振り分けサーバへの接続情報を前記サービスサーバに送信する第1の振り分けサーバと、サービスサーバから前記第2の振り分け情報を受信し、当該第2の振り分け情報に対応する認証サーバへの接続情報を前記サービスサーバに送

信する第2の振り分けサーバと、から構成されるように構成することができる（第7の構成）。

また、本発明は、第7の構成の振り分けシステムから認証サーバへの接続情報を受信するサービスサーバが、端末機器から第1の振り分け情報と、第2の振り分け情報を受信する振り分け情報受信手段と、第1の振り分けサーバに接続し、前記受信した第1の振り分け情報を前記第1の振り分けサーバに送信する第1の送信手段と、前記第1の振り分けサーバから、前記送信した第1の振り分け情報に対応する前記第2の振り分けサーバへの接続情報を受信する第1の受信手段と、前記第2の振り分けサーバに、前記第1の受信手段で受信した接続情報を用いて接続して前記第2の振り分け情報を送信する第2の送信手段と、前記第2の振り分けサーバから、前記送信した第2の振り分け情報に対応する前記認証サーバへの接続情報を受信する第2の受信手段と、前記第2の受信手段で受信した接続情報を前記端末機器に送信する接続情報送信手段と、を具備するように構成することができる（第8の構成）。

また、本発明は、第7の構成の振り分けシステムでサービスサーバに第2の振り分けサーバへの接続情報を提供する第1の振り分けサーバが、サービスサーバから第1の振り分け情報を受信する受信手段と、前記受信した第1の振り分け情報を対応する第2の振り分けサーバへの接続情報を送信する送信手段と、を具備するように構成することができる（第9の構成）。

また、本発明は、第7の構成の振り分けシステムでサービスサーバに認証サーバへの接続情報を提供する第2の振り分けサーバが、サービスサーバから第2の振り分け情報を受信する受信手段と、前記受信した第2の振り分け情報を対応する認証サーバへの接続情報を送信する送信手段と、を具備するように構成することができる（第10の構成）。

また、本発明は、第1の構成の端末機器認証システムでサービスサーバが提供するサービスをコンピュータで利用する端末機器方法であって、前記コンピュータは、第1の受信手段と、第1の送信手段と、第2の受信手段と、第2の送信手段と、第3の受信手段と、認証情報送信手段と、  
5 認証結果受信手段と、認証結果送信手段と、を具備し、前記サービスサーバから、第1の振り分けサーバへの接続情報を前記第1の受信手段で受信する第1の受信ステップと、前記第1の振り分けサーバに、前記第1の受信ステップで受信した接続情報を用いて接続して第1の振り分け情報を前記第1の送信手段で送信する第1の送信ステップと、前記第1の振り分けサーバから、前記送信した第1の振り分け情報をに対応した第2の振り分けサーバへの接続情報を前記第2の受信手段で受信する第2の受信ステップと、前記第2の振り分けサーバに、前記第2の受信ステップで受信した接続情報を用いて接続して第2の振り分け情報を前記第2の送信手段で送信する第2の送信ステップと、前記第2の振り分けサーバから、前記送信した第2の振り分け情報をに対応した認証サーバへの接続情報を前記第3の受信手段で受信する第3の受信ステップと、前記認証サーバに、前記第3の受信ステップで受信した接続情報を用いて接続して認証情報を前記認証情報送信手段で送信する認証情報送信ステップと、前記認証情報送信ステップで送信した認証情報による認証結果を前記認証結果受信手段で前記認証サーバから受信する認証結果受信ステップと、前記認証結果受信ステップで受信した認証結果を前記サービスサーバに前記認証結果送信手段で送信する認証結果送信ステップと、から構成されたことを特徴とする端末機器方法を提供する。

また、本発明は、第1の構成の端末機器認証システムで端末機器に第2の振り分けサーバへの接続情報を提供する第1の振り分け方法であって、受信手段と、送信手段を備えたコンピュータにおいて、前記受信手

段で、端末機器からの接続を受け付け、前記端末機器から第1の振り分け情報を受信する受信ステップと、前記送信手段で、前記受信した第1の振り分け情報を対応する第2の振り分けサーバへの接続情報を前記端末機器に送信する送信ステップと、から構成されたことを特徴とする第5 1の振り分け方法を提供する。

また、本発明は、第4の構成の端末機器認証システムでサービスサーバに認証サーバへの接続情報を提供する振り分け方法であって、振り分け情報受信手段と、接続情報送信手段と、を備えたコンピュータシステムにおいて、前記振り分け情報受信手段で、サービスサーバから振り分け情報を受信する振り分け情報受信ステップと、前記接続情報送信手段で、前記受信した振り分け情報を対応する認証サーバへの接続情報を送信する接続情報送信ステップと、から構成されたことを特徴とする振り分け方法を提供する。

また、本発明は、第4の構成の端末機器認証システムで端末機器にサービスを提供するサービス提供方法であって、振り分け情報受信手段と、振り分け情報送信手段と、接続情報受信手段と、接続情報送信手段と、を備えたコンピュータにおいて、前記振り分け情報受信手段で、端末機器から振り分け情報を受信する振り分け情報受信ステップと、前記振り分け情報送信手段で、前記受信した振り分け情報を振り分けシステムに送信する振り分け情報送信ステップと、前記接続情報受信手段で、前記送信した振り分け情報を対応する認証サーバへの接続情報を前記振り分けシステムから受信する接続情報受信ステップと、前記接続情報送信手段で、前記受信した接続情報を前記端末機器に送信する接続情報送信ステップと、から構成されたことを特徴とするサービス提供方法を提供する。

また、本発明は、第7の構成の振り分けシステムから認証サーバへの接続情報を受信するサービスサーバ方法であって、振り分け情報受信手段と、第1の送信手段と、第1の受信手段と、第2の送信手段と、第2の受信手段と、接続情報送信手段と、を備えたコンピュータにおいて、

5 前記振り分け情報受信手段で、端末機器から第1の振り分け情報と、第2の振り分け情報を受信する振り分け情報受信ステップと、第1の振り分けサーバに接続し、前記受信した第1の振り分け情報を前記第1の送信手段で前記第1の振り分けサーバに送信する第1の送信ステップと、前記第1の振り分けサーバから、前記送信した第1の振り分け情報に対応する前記第2の振り分けサーバへの接続情報を前記第1の受信手段で受信する第1の受信ステップと、前記第2の振り分けサーバに、前記第1の受信ステップで受信した接続情報を用いて接続して前記第2の振り分け情報を、前記第2の送信手段で送信する第2の送信ステップと、前記第2の振り分けサーバから、前記送信した第2の振り分け情報に対応する前記認証サーバへの接続情報を前記第2の受信手段で受信する第2の受信ステップと、前記第2の受信手段で受信した接続情報を前記接続情報送信手段で前記端末機器に送信する接続情報送信ステップと、をから構成されたことを特徴とするサービスサーバ方法を提供する。

また、本発明は、第7の構成の振り分けシステムでサービスサーバに第2の振り分けサーバへの接続情報を提供する第1の振り分け方法であって、受信手段と、送信手段と、を備えたコンピュータにおいて、サービスサーバから第1の振り分け情報を前記受信手段で受信する受信ステップと、前記受信した第1の振り分け情報に対応する第2の振り分けサーバへの接続情報を前記送信手段で送信する送信ステップと、から構成されたことを特徴とする第1の振り分け方法を提供する。

また、本発明は、第7の構成の振り分けシステムでサービスサーバに認証サーバへの接続情報を提供する第2の振り分け方法であって、受信手段と、送信手段と、を備えたコンピュータにおいて、サービスサーバから第2の振り分け情報を前記受信手段で受信する受信ステップと、前記受信した第2の振り分け情報に対応する認証サーバへの接続情報を前記送信手段で送信する送信ステップと、から構成されたことを特徴とする第2の振り分け方法を提供する。

また、本発明は、第1の構成の端末機器認証システムでサービスサーバが提供するサービスを利用するコンピュータで構成された端末機器において、前記サービスサーバから、第1の振り分けサーバへの接続情報を受信する第1の受信機能と、前記第1の振り分けサーバに、前記第1の受信機能で受信した接続情報を用いて接続して第1の振り分け情報を送信する第1の送信機能と、前記第1の振り分けサーバから、前記送信した第1の振り分け情報を対応した第2の振り分けサーバへの接続情報を受信する第2の受信機能と、前記第2の振り分けサーバに、前記第2の受信機能で受信した接続情報を用いて接続して第2の振り分け情報を送信する第1の送信機能と、前記第2の振り分けサーバから、前記送信した第2の振り分け情報を対応した認証サーバへの接続情報を受信する第3の受信機能と、前記認証サーバに、前記第3の受信機能で受信した接続情報を用いて接続して認証情報を送信する認証情報送信機能と、前記認証情報送信機能で送信した認証情報による認証結果を前記認証サーバから受信する認証結果受信機能と、前記認証結果受信機能で受信した認証結果を前記サービスサーバに送信する認証結果送信機能と、を実現する端末機器プログラムを提供する。

また、本発明は、第1の構成の端末機器認証システムで端末機器に第2の振り分けサーバへの接続情報を提供するコンピュータで構成された

第 1 の振り分けサーバにおいて、端末機器からの接続を受け付け、前記端末機器から第 1 の振り分け情報を受信する受信機能と、前記受信した第 1 の振り分け情報に対応する第 2 の振り分けサーバへの接続情報を前記端末機器に送信する送信機能と、を実現する第 1 の振り分けプログラムを提供する。  
5

また、本発明は、第 4 の構成の端末機器認証システムでサービスサーバに認証サーバへの接続情報を提供するコンピュータから構成された振り分けシステムにおいて、サービスサーバから振り分け情報を受信する振り分け情報受信機能と、前記受信した振り分け情報に対応する認証サーバへの接続情報を送信する接続情報送信機能と、を実現する振り分けプログラムを提供する。  
10

また、本発明は、第 4 の構成の端末機器認証システムで端末機器にサービスを提供するコンピュータで構成されたサービスサーバにおいて、端末機器から振り分け情報を受信する振り分け情報受信機能と、前記受信した振り分け情報を振り分けシステムに送信する振り分け情報送信機能と、前記送信した振り分け情報に対応する認証サーバへの接続情報を前記振り分けシステムから受信する接続情報受信機能と、前記受信した接続情報を前記端末機器に送信する接続情報送信機能と、を実現するサービスサーバプログラムを提供する。  
15

また、本発明は、第 7 の構成の振り分けシステムから認証サーバへの接続情報を受信するコンピュータで構成されたサービスサーバにおいて、端末機器から第 1 の振り分け情報と、第 2 の振り分け情報を受信する振り分け情報受信機能と、第 1 の振り分けサーバに接続し、前記受信した第 1 の振り分け情報を前記第 1 の振り分けサーバに送信する第 1 の送信機能と、前記第 1 の振り分けサーバから、前記送信した第 1 の振り分け情報に対応する前記第 2 の振り分けサーバへの接続情報を受信する第 1  
20  
25

の受信機能と、前記第2の振り分けサーバに、前記第1の受信機能で受信した接続情報を用いて接続して前記第2の振り分け情報を送信する第2の送信機能と、前記第2の振り分けサーバから、前記送信した第2の振り分け情報に対応する前記認証サーバへの接続情報を受信する第2の受信機能と、前記第2の受信機能で受信した接続情報を前記端末機器に送信する接続情報送信機能と、を実現するサービスサーバプログラムを提供する。

また、本発明は、第7の構成の振り分けシステムでサービスサーバに第2の振り分けサーバへの接続情報を提供するコンピュータで構成された第1の振り分けサーバにおいて、サービスサーバから第1の振り分け情報を受信する受信機能と、前記受信した第1の振り分け情報に対応する第2の振り分けサーバへの接続情報を送信する送信機能と、を実現する第1の振り分けプログラムを提供する。

また、本発明は、第7の構成の振り分けシステムでサービスサーバに認証サーバへの接続情報を提供するコンピュータで構成された第2の振り分けサーバにおいて、サービスサーバから第2の振り分け情報を受信する受信機能と、前記受信した第2の振り分け情報に対応する認証サーバへの接続情報を送信する送信機能と、を実現する第2の振り分けプログラムを提供する。

また、本発明は、上記各プログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する。

更に、本発明は、第2の構成に係る端末機器を、前記第3の受信手段で受信した認証サーバへの接続情報を記憶する接続情報記憶手段と、前記サービスサーバから前記第1の振り分けサーバへの接続情報を受信した場合に前記接続情報記憶手段で前記接続情報を記憶しているか否かを確認する確認手段と、を具備し、前記確認手段で前記接続情報が記憶さ

れていることが確認された場合、前記認証情報送信手段は、前記記憶されている接続情報を用いて前記認証サーバに接続して認証情報を送信するように構成することもできる（第11の構成）。

更に、第11の構成の端末機器を、前記認証情報送信手段が、前記接続情報記憶手段で記憶している前記接続情報を用いて前記認証サーバに接続できなかった場合、前記第1の受信手段で受信した接続情報を元に、前記第1の送信手段、前記第2の受信手段、前記第2の送信手段、及び前記第3の受信手段を用いて取得される認証サーバの接続情報を用いて前記認証サーバに接続して認証情報を送信し、前記接続情報記憶手段が、前記取得した認証サーバへの接続情報を用いて、記憶してある接続情報を更新するように構成することもできる（第12の構成）。

本発明によれば、CE機器の認証先を適切に振り分けることができる。

#### 図面の簡単な説明

15 第1図は、本実施の形態の機器認証システムのネットワーク構成を示した図である。

第2図は、機器IDの論理的な構成の一例を示した図である。

第3図は、第1の実施形態におけるCE機器と各サーバとの関係を説明するための図である。

20 第4図は、第1の実施形態でサービスサーバが認証を要するサービスを提供する手順を説明するためのフローチャートである。

第5A図乃至第5B図は、機器認証トリガとして使用されるプロトコルの一例を示した図である。

25 第6図は、第2の実施形態におけるCE機器と各サーバとの関係を説明するための図である。

第7図は、第2の実施形態でサービスサーバが認証を要するサービスを提供する手順を説明するためのフローチャートである。

第8図は、未公開の特許文献によるCE機器の認証システムの構成を示した図である。

5

#### 発明を実施するための最良の形態

以下、本発明の好適な実施の第1の実施形態、及び第2の実施形態について、図を参照して詳細に説明する。

##### [第1の実施形態の概要]

10 CE機器3は、第2図に示したように企業を特定する企業情報15と企業が自由に設定できる付属情報16からなる機器ID13を記憶している。

15 第3図において、サービスサーバ10は、CE機器3に機器認証を要するサービスを提供する場合、CE機器3に企業情報振り分けサーバ6への接続情報を送信する。

CE機器3は、この接続情報を用いて企業情報振り分けサーバ6に企業情報15を送信する。

企業情報振り分けサーバ6は、この企業情報15を振り分けサーバテーブル21で検索し、認証先振り分けサーバ8への接続情報を取得する。

20 振り分けサーバテーブル21では、企業情報15と、各企業ごとに運営されている認証先振り分けサーバ8が対応付けられている。そして、企業情報振り分けサーバ6は、取得した接続情報をCE機器3に送信する。

CE機器3は、この接続情報を用いて当該企業が運営する認証先振り分けサーバ8に接続し、機器ID13を送信する。

25 認証先振り分けサーバ8は、機器ID13を認証サーバテーブル22で検索し、CE機器3の認証を担当する認証サーバ9への接続情報を取

得する。認証サーバテーブル 2 2 では、各機器 I D 1 3 と、その C E 機器 3 の認証を担当する認証サーバ 9 が対応付けられている。これは、同じ企業の C E 機器 3 でも、 C E 機器 3 によって認証サーバ 9 を複数用意している場合があるからである。そして、認証先振り分けサーバ 8 は、

5 取得した接続情報を C E 機器 3 に送信する。

C E 機器 3 は、この接続情報により自己の認証を担当している認証サーバ 9 を特定することができる。

C E 機器 3 は、この接続情報を用いて認証サーバ 9 に接続し、パスフレーズ、機器 I D 1 3 など、機器認証に必要な認証情報を送信する。

10 これに応じて認証サーバ 9 は、 C E 機器 3 の機器認証を行う。

このように本実施の形態では、 C E 機器 3 は、企業情報振り分けサーバ 6 に接続すべき認証先振り分けサーバ 8 を問い合わせ、更に、認証先振り分けサーバ 8 に接続すべき認証サーバ 9 を問い合わせせる。

15 このとき、企業情報振り分けサーバ 6 では企業情報による接続先の振り分けが行われ、認証先振り分けサーバ 8 では機器 I D 1 3 による振り分けが行われる。

このように、企業情報振り分けサーバ 6 に接続するまでは、各企業に共通の処理を行い、企業情報振り分けサーバ 6 から認証先振り分けサーバ 8 への接続情報を受信した後の処理は各企業が独自に設定することができる。

#### [第 1 の実施形態の詳細]

第 1 図は、本実施の形態の機器認証システム 1 のネットワーク構成を示した図である。

機器認証システム 1 は、 C E 機器 3 、企業情報振り分けサーバ 6 、認

25 証先振り分けサーバ 8 a 、 8 b 、 8 c 、 … 、認証サーバ 9 a 、 9 b 、 9

c、…、サービスサーバ10などがインターネット5を介して接続可能に配設されている。

第1図中では、CE機器3、サービスサーバ10はそれぞれ1つのみ記載されているが、これらは複数存在する。また、企業情報振り分けサーバ6は、機器認証システム1中に1台存在する。

なお、以下では、認証先振り分けサーバ8a、8b、8c、…を特に区別しない場合は単に認証先振り分けサーバ8と記す。同様に認証サーバ9a、9b、9c、…、に対しても区別しない場合は単に認証サーバ9と記す。

CE機器3は、例えば、テレビやビデオ、レコーダ、オーディオ、ゲーム機、PDA、炊飯器、エアコンなどの電機製品で構成されたCE機器である。

CE機器3には、通信機能を有したコンピュータが内蔵されており、インターネット5を介して各種サーバ（サービスサーバ10、企業情報振り分けサーバ6、認証先振り分けサーバ8、認証サーバ9、その他のサーバ）と通信することができ、端末機器を構成している。

CE機器3は、個体を他のCE機器から区別するための機器IDを記憶しており、通信先のサーバは、CE機器3から機器IDを受信することによりCE機器3を識別することができる。

後述するように、機器IDは、CE機器3の製造、又は販売元の企業を表す企業情報と、各企業が自由に設定することができる付属情報から構成されている。

また、CE機器3は、機器認証を行うためのバスフレーズも記憶しており、機器認証の際に使用される。

パスフレーズは、パスワードと同様の機能を果たす文字列であり、パスワードより長いものをパスフレーズと呼んでいるが、機器認証を行なうために用いられるのは、パスフレーズでもパスワードでも良い。

サービスサーバ10は、CE機器3にサービスを提供するためのサービスサイトが開設されたサーバである。

サービスサーバ10は、サービスサイトにアクセスしてきたCE機器3に対して、コンテンツを送信したり、サービスを提供する。ユーザは、CE機器3でこのコンテンツを利用したり、サービス提供を受けたり、サービスサーバ10の提供するサービスを利用することができる。

サービスサーバ10が提供するコンテンツは、例えば、音楽コンテンツ、旅行情報コンテンツ、映画コンテンツ、レシピコンテンツなどがある。

サービスサーバ10が提供するサービスは、例えば、趣味・嗜好を含む個人情報やCE機器の機器情報、インターネット接続用設定パラメータ等の情報提供、CE機器のメンテナンスや、ソフトウェアのアップデート等を含む。また、他には、オンラインストレージサービスや、アフィニティサービス（機器の仕様とサービスと、他の機器からの要求仕様やサービスとのマッチングサービス）も提供可能とする。

また、CE機器3が便器であり、ユーザの便をセンサでセンシングして健康状態をチェックするというようなサービスを提供することもできる。

サービスサーバ10が提供するサービスには、機器認証を要さずに提供できるものと、機器認証を要するものがある。

CE機器3が機器認証を要するサービスを要求した場合、サービスサーバ10は、企業情報振り分けサーバ6に接続するようにCE機器3に要求する。

ここで、CE機器3が機器認証を要するサービスを要求する場合の例として、CE機器3を内蔵したステレオ装置に音楽データを送信するサービスについて説明する。

まず、サービスサーバ10は、ステレオ装置に音楽を選択する選択画面を表示するための画面データを送信する。この選択画面データは、例えば、HTML (Hyper text Markup Language)などのコンピュータ言語により記述されている。

そして、ステレオ装置は、この画面データを用いてステレオ装置が備えたディスプレイ上に音楽を選択するための選択画面を表示する。

選択画面では、ダウンロードする楽曲を、音楽のジャンル、アーティスト名、楽曲名など、段階的に楽曲を絞り込むことができるようになっている。

この絞り込み操作は、機器認証せずに行うことができ、ユーザが絞り込むごとに応する画面が表示される。

楽曲を絞り込んだ後、これをダウンロードする段階は機器認証が必要となるように設定されている。これは、選択画面に表示されたダウンロードボタンに対応して、機器認証を要する操作を行おうとしていることをサービスサーバ10に通知するタグを画面データに埋め込んでおくことにより実現することができる。

これにより、ユーザがダウンロードボタンをクリックすると、CE機器3からサービスサーバ10に機器認証が必要であるとの通知が送信され、これに対してサービスサーバ10は、CE機器3に機器認証を行わせるきっかけとなる情報（機器認証トリガと呼ぶことにする）を送信する。

CE機器3は、機器認証トリガをサービスサーバ10から受信し、これにより一連の認証動作を行うことになる。機器認証トリガには、企業

情報振り分けサーバ6への接続情報が含まれており、CE機器3は、これを用いて企業情報振り分けサーバ6に接続することができる。

企業情報振り分けサーバ6は、CE機器3に接続先の認証先振り分けサーバ8を指示するサーバである。

5 企業情報振り分けサーバ6は、企業情報と認証先振り分けサーバ8を対応させた振り分けサーバテーブルを記憶しており、CE機器3から機器IDに含まれる企業情報を受信して、接続すべき認証先振り分けサーバ8の接続情報をCE機器3に送信する。

10 認証先振り分けサーバ8は、各企業ごとに設けられており、CE機器3に接続先の認証サーバ9を指示するサーバである。

認証先振り分けサーバ8は、機器IDと認証サーバ9を対応させた認証サーバテーブルを記憶しており、CE機器3から機器IDを受信して、接続すべき認証サーバ9の接続情報をCE機器3に送信する。

15 認証サーバ9は、CE機器3の機器認証を行うサーバ装置である。認証サーバ9は、1企業につき、単数又は複数用意されている。認証サーバ9は、CE機器3の機器IDとパスフレーズに基づいて機器認証を行う。

20 なお、以上の企業情報振り分けサーバ6、認証先振り分けサーバ8、認証サーバ9、サービスサーバ10のサービスサイトは、URL (U n i form R esource L ocators) やURI (U n i que R esource I dent i fier) などによりインターネット上で特定することができる。

そして、CE機器3が各サーバとやり取りする接続情報には、これらURL、URIなどが含まれており、CE機器3は、これらの情報を用いて所定のサーバに接続する。

即ち、接続情報は、例えば「`http://abc.Zony.co.jp`」といったような、CE機器3の接続先（企業情報振り分けサーバ6、認証先振り分けサーバ8、認証サーバ9など）を特定するための情報が含まれている。

5 また、CE機器3や各サーバが送受信するデータは全て暗号化されており、第三者の不正アクセスを防止するようになっている。

10 このように、企業情報振り分けサーバ6、及び認証先振り分けサーバ8は、それぞれ第1の振り分けサーバと第2の振り分けサーバを構成しており、CE機器3に対し、サービスサーバ10は、企業情報振り分けサーバ6への接続情報を送信し、企業情報振り分けサーバ6は、認証先振り分けサーバ8への接続情報を送信し、認証先振り分けサーバ8は、認証サーバ9への接続情報を送信する。

第2図は、CE機器3が備えた機器ID13の論理的な構成の一例を示した図である。

15 機器ID13は、企業を特定する企業情報15と、各企業が自由に設定することができる付属情報16から構成されている。

付属情報16は、例えば、CE機器3のシリアルナンバ、CE機器3の種類、製造年月日など、各種の情報を含めることができ、本実施の形態では一例としてCE機器3のシリアルナンバが含まれているものとする。このシリアルナンバによりCE機器3の個体を特定することができる。

機器ID13として具体的には、IEEE（米国電気電子技術者協会）が管理しているEUI-64（Extended Unique Identifier、64bit）などを採用することができる。

25 EUI-64は、64ビットの情報でCE機器3を管理する規格である。

特に全 64 ビットのうち、上位 24 ビットは OUI (Organizationally Unique Identifier) と呼ばれ、IEEE が各企業（ベンダー）に支給するコードである。本実施の形態では OUI が企業情報 15 に対応する。

5 OUI 以外の下位 40 ビットは、各企業が自由に管理することができ、本実施の形態の付属情報 16 に対応する。

本実施の形態では、企業情報 15 は、企業情報振り分けサーバ 6 が認証先振り分けサーバ 8 の接続情報を取得するために用いる第 1 の振り分け情報を構成し、機器 ID 13 は、認証先振り分けサーバ 8 が認証サーバ 9 の接続情報を取得するために用いる第 2 の振り分け情報を構成している。

第 3 図は、CE 機器 3 と各サーバとの関係を説明するための図である。

CE 機器 3 がサービスサーバ 10 からサービスを受けるまでの段階をステップごとに説明する。

15 ステップ 1 : CE 機器 3 がサービスサーバ 10 に対して、機器認証を要するサービスを要求すると、サービスサーバ 10 は、企業情報振り分けサーバ 6 に接続するための接続情報を送信する。

20 ステップ 2 : CE 機器 3 は、この接続情報を用いて企業情報振り分けサーバ 6 に接続し、企業情報振り分けサーバ 6 に企業情報 15 を送信する。

企業情報振り分けサーバ 6 は、各企業情報 15 と、認証先振り分けサーバ 8 に接続するための接続情報を対応させた振り分けサーバテーブル 21 を備えている。振り分けサーバテーブル 21 により、CE 機器 3 と各企業が運営する認証先振り分けサーバ 8 がひもづけられている。

企業情報振り分けサーバ6は、CE機器3から受信した企業情報15をキーとして振り分けサーバテーブル21を検索し、その結果得られた認証先振り分けサーバ8の接続情報をCE機器3に送信する。

ステップ3：CE機器3は、企業情報振り分けサーバ6から受信した5接続情報を用いて、各認証先振り分けサーバ8のうち、CE機器3を担当する自社の認証先振り分けサーバ8に接続する。

そして、CE機器3は自己の機器ID13を読み出して認証先振り分けサーバ8に送信する。

認証先振り分けサーバ8は、機器ID13と、CE機器3の認証を担当する認証サーバ9の接続情報を対応付けた認証サーバテーブル22を備えている。

認証サーバテーブル22により、各CE機器3と各認証サーバ9がひもづけられている。

なお、本実施の形態では、CE機器3の個々に対して認証サーバ9を対応付ける構成としたが、これに限定せず、例えば、CE機器3の型番ごとなど、更に大きな分類ごとに対応付けてもよい。例えば、型番○○○のCE機器3は、接続情報1で特定される認証サーバ9で認証し、型番△△△のCE機器3は、接続情報2で特定される認証サーバ9で認証するといようにすることができる。即ち、CE機器3と認証サーバ9の20対応付けは、各企業が自由に行うことができる。

認証先振り分けサーバ8は、CE機器3から受信した機器ID13をキーとして認証サーバテーブル22を検索し、その結果得られた認証サーバ9の接続情報をCE機器3に送信する。

ステップ4：CE機器3は、企業情報振り分けサーバ6から認証サーバ9への接続情報を受信し、これを用いて認証サーバ9に接続する。そ

して、CE機器3は、パスフレーズや機器ID13など、機器認証に必要な認証情報を認証サーバ9に送信する。

認証サーバ9は、機器ID13と認証情報を対応付けた認証情報テーブル23を備えており、CE機器3から受信した認証情報と認証情報テーブル23の認証情報を対比して機器認証を行う。そして、認証サーバ9は、認証結果をCE機器3に送信する。

ステップ5：CE機器3は、認証サーバ9から受信した認証結果をサービスサーバ10に送信し、サービスの提供を要求する。

サービスサーバ10は、認証結果を受信してCE機器3の認証結果を判断し、CE機器3が認証サーバ9により認証された場合はCE機器3にサービスを提供し、認証されていない場合はその旨のアラームをCE機器3に送信し、サービスの提供は行わない。

第4図は、機器認証システム1でサービスサーバ10がCE機器3に認証を要するサービスを提供する手順を説明するためのフローチャートである。

また、CE機器3、企業情報振り分けサーバ6は、フローチャート中に四角で囲ったような各手順を備えている。

まず、CE機器3がサービスサーバ10に認証を要するサービスの提供を要求する（ステップ5）。

これに対し、サービスサーバ10は、機器認証トリガをCE機器3に送信し、企業情報振り分けサーバ6への接続を指示する（ステップ50）。

CE機器3は、サービスサーバ10から機器認証トリガを受信し（第1の受信手段）、企業情報振り分けサーバ6に接続する。そして、CE機器3は、自己に設定されている機器ID13を読み出し、更にこの機器ID13から企業情報15を取得して企業情報振り分けサーバ6に送

信する（第1の送信手段）。これにより、CE機器3は、企業情報振り分けサーバ6に対してどの認証先振り分けサーバ8に接続したらよいのかの確認を要求する（ステップ10）。

企業情報振り分けサーバ6は、CE機器3から企業情報15を受信し  
5 (受信手段)、これをキーとして振り分けサーバテーブル21からCE  
機器3が接続すべき認証先振り分けサーバ8への接続情報を検索する。  
そして検索された接続情報をCE機器3に送信する（送信手段）（ステ  
ップ70）。

CE機器3は、企業情報振り分けサーバ6から接続情報を受信し（第  
10 2の受信手段）、これを用いて認証先振り分けサーバ8に接続する。そ  
して、CE機器3は、認証先振り分けサーバ8に機器ID13を送信し  
(第2の送信手段)、どの認証サーバ9に接続したらよいのかの確認を要  
求する（ステップ15）。

これに対し、認証先振り分けサーバ8は、CE機器3から機器ID1  
15 3を受信し、これをキーとして認証サーバテーブル22からCE機器3  
が接続すべき認証サーバ9への接続情報を検索する。そして検索された  
接続情報をCE機器3に送信する（送信手段）（ステップ80）。

次に、CE機器3は、認証先振り分けサーバ8から受信した認証サー  
バ9への接続情報を用いて認証サーバ9に接続する。そして、CE機器  
20 3は、認証情報を認証サーバ9に送信し（認証情報送信手段）、認証サ  
ーバ9から認証結果を受信する（認証情報受信手段）。このように、CE  
機器3と認証サーバ9は通信しながら共に一連の機器認証シーケンス  
を行う（ステップ20、ステップ93）。

この機器認証シーケンスは、例えば、機器ID13やパスフレーズな  
25 どの認証情報を認証サーバ9に送信し、認証サーバ9が認証情報テーブ  
ル23でこれを確認することにより行う。

また、機器認証に伴うデータの送受信を行う前に、例えば、S S L (S e c u r e S o c k e t s L a y e r) などの暗号技術を用いてC E 機器 3 と認証サーバ 9 の回線接続のセキュリティを確保するように構成してもよい。S S L により通信経路が暗号化され、セキュリティの高い通信を行うことができる。

認証サーバ 9 は、C E 機器 3 から受信した認証情報により認証結果をC E 機器 3 に送信する（ステップ 9 5）。このとき、認証サーバ 9 は、サービスサーバ 1 0 が後に、C E 機器 3 が確かに認証サーバ 9 で認証されたことを確認するためのワンタイムパスワードを発行し、これもC E 機器 3 に送信する。

このワンタイムパスワードを発行することにより、認証サーバ 9 と同様な機能を有する偽造サーバなどのなりすましを防止することができる。

認証サーバ 9 は、発行したワンタイムパスワードと、発行対象であるC E 機器 3 の機器 I D 1 3 を対応付けて記憶しておく。

C E 機器 3 は、認証サーバ 9 から受信した認証結果とワンタイムパスワードをサービスサーバ 1 0 に送信し（認証結果送信手段）、サービスの提供を要求する（ステップ 2 5）。この場合も、S S L などの暗号化技術を用いて回線接続のセキュリティを高めることができる。

そして、サービスサーバ 1 0 は、C E 機器 3 から認証結果、機器 I D 1 3、及びワンタイムパスワードを受信する。

そして、サービスサーバ 1 0 は、受信した機器 I D 1 3 とワンタイムパスワードを認証サーバ 9 に送信し、C E 機器 3 から受信した認証結果が確かに認証サーバ 9 が発行したものであるかの認証の確認を認証サーバ 9 に要求する（ステップ 5 5）。

認証サーバ 9 は、サービスサーバ 1 0 から機器 I D 1 3 とワンタイムパスワードを受信し、先にステップ 9 5 で対応付けていた機器 I D 1 3

とワンタイムパスワードと照合し、確かに認証サーバ9が行った認証であることを確認する。そして認証確認結果をサービスサーバ10に送信する（ステップ98）。

なお、以上のステップ55、及びステップ98でのサービスサーバ10と認証サーバ9との通信は、SSLなどの暗号化技術を用いてセキュリティを高めることができる。

サービスサーバ10は、認証サーバ9から認証確認結果を受信し、CE機器3から送信されてきた認証結果が確かに認証サーバ9が発行したものであることを確認し、更に、CE機器3から受信した認証結果がCE機器3の認証を証明するものであった場合に、CE機器3に対するサービスの提供を開始する（ステップ60）。

CE機器3は、サービスサーバ10からコンテンツなどのサービス対象を受信し、ユーザがこれを利用する（ステップ30）。

なお、ステップ60において、認証サーバ9からの認証の確認が取れなかった場合、あるいは、CE機器3から受信した認証結果が、CE機器3の認証を認めないものであった場合、サービスサーバ10は、CE機器3に対してサービスの提供を行わない。

第5A図乃至第5B図は、機器認証トリガとして使用されるプロトコルの一例を示した図である。

第5A図は、従来の機器認証で使用されていたプロトコルであり、認証サーバのURL31と、認証サーバで提供しているサービス（認証サービス）の名称32、認証が成功した後にCE機器3が接続するサイトのURL33、認証されなかった場合に接続する接続先のURL34、及び機器認証バージョン35が含まれている。

機器認証にはいくつかのバージョンが用意されており、認証されるバージョンによってサービスサーバで利用されるサービスが異なる。機器認証バージョン 3 5 は、これを表している。

5 このように、従来のプロトコルには認証サーバへの接続情報（URL）が含まれており、CE 機器 3 は、これを用いて認証サーバに接続する。

第 5 B 図は、本実施の形態で機器認証トリガとして使用するプロトコルの一例を示している。

10 このプロトコルには、プライマリ用プロトコル 4 1 とセカンダリ用プロトコル 5 0 が用意されている。

通常はプライマリ用プロトコル 4 1 を用いて企業情報振り分けサーバ 6 に接続するが、企業情報振り分けサーバ 6 に障害が発生していたり、あるいは企業情報振り分けサーバ 6 が混雑していたりなどして企業情報振り分けサーバ 6 に接続できない場合にセカンダリ用プロトコル 5 0 を用いて予備の企業情報振り分けサーバ 6 に接続するようになっている。

15 基本的にプライマリ用プロトコル 4 1 とセカンダリ用プロトコル 5 0 は、同等の情報から構成されている。

20 プライマリ用プロトコル 4 1 には、企業情報振り分けサーバ 6 の URL 4 2 と、企業情報振り分けサーバ 6 で提供しているサービス（振り分けサービス）の名称 4 3 、認証が成功した後に CE 機器 3 が接続するサイトの URL 4 4 、認証されなかった場合に接続する接続先の URL 4 5 、及び機器認証バージョン 4 6 が含まれている。

25 このように、プライマリ用プロトコル 4 1 には、企業情報振り分けサーバ 6 への接続情報（URL）が含まれており、CE 機器 3 は、これを用いて企業情報振り分けサーバ 6 に接続する。

以上に説明した第1の実施形態では、以下のような効果を得ることができる。

(1) 機器認証先をCE機器3の認証を管轄する企業ごとに振り分け、更に、振り分け先で個々の認証サーバ9に振り分けることができる。

5 (2) 機器認証には、各企業ごとに独自に設定されている機密情報を用いて行う場合が多い。そして、全ての機器認証対応製品の情報が1つの機器認証先振り分けサーバに集中すると各社の機密情報や製品生産情報（機器ID13から何台生産したのかわかつてしまう）が他社に漏れる可能性がある。しかし、本実施の形態で各企業が共通して利用するのは、企業情報を用いて認証先を振り分ける企業情報振り分けサーバ6だけとすることができますので、機密情報の管理が容易であり、セキュリティも高い。

10 (3) 認証サーバ9発見のための時間とコストを削減することができる。

15 (4) 認証サーバ9を決定するための決定プロトコルと認証サーバ9での認証プロトコルを分離することによって様々な認証方式や独自認証方式にオープンに対応することができる。

20 (5) CE機器3から企業情報振り分けサーバ6へのコンタクトでは、企業情報振り分けサーバ6にパスフレーズや機器ID13を送信する必要が無く、セキュリティを高めることができる。

(6) CE機器3から認証先振り分けサーバ8へのコンタクトでは、認証先振り分けサーバ8にパスフレーズを送信する必要が無く、セキュリティを高めることができる。

25 なお、本実施の形態では、サービスサーバ10から認証トリガに認証サーバ9への接続情報を含まない場合、即ち、認証サーバ9を指定していない場合について説明したが、これに限定せず、認証サーバ9が指定

されていない場合のみ振り分けフェーズに入り、指定されている場合は振り分けをバイパスして C E 機器 3 から直接認証サーバ 9 に認証を受けに行くように構成することもできる。

また、今後 C E 機器 3 の普及が見込まれ、機器認証システム 1 は、機器認証標準化スキームの基本方式として採用することができる。

これまで、本実施の形態として、企業情報振り分けサーバ 6 及び認証先振り分けサーバ 8 において、 C E 機器 3 を認証するための認証サーバ 9 を振り分けていたが、一度企業情報振り分けサーバ 6 及び認証先振り分けサーバ 8 によって、 C E 機器 3 が認証サーバ 9 の接続情報を取得していればこれを記憶しておき（接続情報記憶手段）、 C E 機器 3 は、企業情報振り分けサーバ 6 及び認証先振り分けサーバ 8 への接続をスキップして、記憶されている認証サーバ 9 の接続情報を読み出して、認証サーバ 9 に接続してもよい。

CE 機器が直接認証サーバ 9 に接続するためには、サービスサーバ 10 から受信する機器認証トリガに振り分けサービス対応であることが分かるような情報が必要である。具体的には、第 5 B 図のサービスの名称 43 に、振り分けサービスを特定する Object ID を、例えば、 DADP (Device Authentication Service Discovery Protocol) などと、記述しておく必要がある。

CE 機器 3 は、機器認証トリガに振り分けサービスを特定する Object ID を読み出すと、これより前に振り分けサービスによって振り分けられた、 C E 機器 3 を認証する認証サーバ 9 の接続情報を持っているか否かを確認する（確認手段）。もし、認証サーバ 9 の接続情報を既に持つていれば、 C E 機器 3 は、企業情報振り分けサーバ 6 及び認証先

振り分けサーバ8に接続することなく、直接認証サーバ9へ接続して、認証を行う。

CE機器3が既に知っている認証サーバ9の接続情報先にアクセスしても、認証サーバ9が変わっていた場合にはエラー処理が発生する。この5ような場合には、上述したステップによる振り分けサービスを利用し、認証サーバ9の接続情報を取得する。

CE機器3が、認証サーバ9から認証確認を受けとると、認証先振り分けサーバ8から受信される認証サーバの接続情報をキャッシュする(更新する)。

10 上述したとおり、本実施形態においては、CE機器3は、企業情報振り分けサーバ6に、第2図に示される構成の機器ID13を送信しているが、機器IDすべての情報を出さずに、例えば、企業情報振り分けサーバ6には、CE機器3がどこの企業に製造されたCE機器であるかの情報、すなわち、企業情報15のみを送信してもよい。

15 また、付属情報16は更に、機器種別情報16-1と機器固体識別情報16-2とから構成されていれば、認証先振り分けサーバ8には機器種別情報16-1のみを送信し、認証サーバ9にのみ機器ID13を送信することとしてもよい。機器IDすべてを送信するか、必要最低限の一部を送信するかについては、少なくとも、企業情報振り分けサーバ6および認証先振り分けサーバ8が、次の接続先を決定できるに足る情報量があればよい。

機器IDの必要な情報量を決めるのは、サービスサーバ10および企業情報振り分けサーバ6が、それぞれ、企業情報振り分けサーバ6および認証先振り分けサーバ8が必要とする情報量を、CE機器3に指定してもよい。また、企業情報振り分けサーバ6および認証先振り分けサー

バ8が、あらかじめCE機器3に、接続時に必要とされる機器IDの情報量を知らせておくことも可能である。

機器IDの一部を指定するのは、上位何ビットが必要であると特定してもよいし、必要な箇所のみの情報を得るマスク情報を与え、マスク情報と機器ID13とを演算した結果取得してもよい。例えば、機器ID13が、企業情報15として“1010”、付属情報16として“110001101”から構成され、企業情報15のみを必要とするならば、マスク情報として“1111000000000”を与え、機器IDとマスク情報の論理積を“1010000000000”を送信する情報としてもよい。機器IDの一部を指定する方法はこれに限るものではなく、必要なデータのみが分かる形態であればよい。

#### 〔第2の実施形態の概要〕

第6図において、CE機器3は、サービスサーバ10に機器認証を要するサービスの提供を要求する場合、サービスサーバ10に機器ID13を送信する。

サービスサーバ10は、この機器ID13から企業情報15を抽出し、企業情報振り分けサーバ6に送信する。

企業情報振り分けサーバ6は、この企業情報15を振り分けサーバテーブル21で検索し、認証先振り分けサーバ8への接続情報を取得する。

そして、企業情報振り分けサーバ6は、取得した接続情報をサービスサーバ10に送信する。

サービスサーバ10は、この接続情報を用いてCE機器3の企業が運営する認証先振り分けサーバ8に接続し、機器ID13を送信する。

認証先振り分けサーバ8は、機器ID13を認証サーバテーブル22で検索し、CE機器3の認証を担当する認証サーバ9への接続情報を取

得する。そして、認証先振り分けサーバ8は、取得した接続情報をサービスサーバ10に送信する。

サービスサーバ10は、この接続情報をCE機器3に送信する。

CE機器3は、この接続情報により自己の認証を担当している認証サーバ9を特定することができる。

CE機器3は、この接続情報を用いて認証サーバ9に接続し、パスフレーズ、機器ID13など、機器認証に必要な認証情報を送信する。

これに応じて認証サーバ9は、CE機器3の機器認証を行う。

このように本実施の形態では、機器ID13による認証サーバ9の特定をサービスサーバ10が行う。

#### [第2の実施形態の詳細]

本実施の形態のネットワーク構成は、第1の実施形態（第1図）と同様である。以下では、対応する構成要素には同じ符号を付して説明する。また、本実施の形態のCE機器3が使用する機器IDは、第2図に示したものと同様である。

第6図は、CE機器3と機器認証システム1を構成する各サーバとの関係を説明するための図である。

CE機器3がサービスサーバ10からサービスを受けるまでの段階をステップごとに説明する。

20 ステップ1：CE機器3がサービスサーバ10に対して、機器認証を要するサービスを要求する。そして、要求に伴って自身の機器ID13を読み出し、サービスサーバ10に送信する。

25 ステップ2：サービスサーバ10は、CE機器3から機器ID13を受信し、機器ID13から企業情報15を抽出して企業情報振り分けサーバ6に送信する。

企業情報振り分けサーバ6は、第1の実施形態と同様に各企業情報15と認証先振り分けサーバ8に接続するための接続情報を対応させた振り分けサーバテーブル21を備えている。振り分けサーバテーブル21により、CE機器3と各企業が運営する認証先振り分けサーバ8がひもづけられている。

企業情報振り分けサーバ6は、サービスサーバ10から受信した企業情報15をキーとして振り分けサーバテーブル21を検索し、その結果得られた認証先振り分けサーバ8の接続情報をサービスサーバ10に送信する。

10 ステップ3：サービスサーバ10は、企業情報振り分けサーバ6から受信した接続情報を用いて、各認証先振り分けサーバ8のうち、当該CE機器3を担当する認証先振り分けサーバ8に接続する。

そして、サービスサーバ10はCE機器3から受信した機器ID13を認証先振り分けサーバ8に送信する。

15 認証先振り分けサーバ8は、第1の実施形態と同様に機器ID13と当該CE機器3の認証を担当する認証サーバ9の接続情報を対応付けた認証サーバテーブル22を備えている。

認証サーバテーブル22により、各CE機器3と各認証サーバ9がひもづけられている。

20 認証先振り分けサーバ8は、CE機器3から受信した機器ID13をキーとして認証サーバテーブル22を検索し、その結果得られた認証サーバ9の接続情報をサービスサーバ10に送信する。

ステップ4：サービスサーバ10は、認証先振り分けサーバ8から、CE機器3の認証を端とする認証サーバ9への接続情報を受信し、これをCE機器3に送信する。

ステップ5：CE機器3は、サービスサーバ10から認証サーバ9への接続情報を受信し、これを用いて認証サーバ9に接続する。そして、CE機器3は、パスフレーズや機器ID13など、機器認証に必要な認証情報を認証サーバ9に送信する。

5 認証サーバ9は、第1の実施形態と同様に機器ID13と認証情報を対応付けた認証情報テーブル23を備えており、CE機器3から受信した認証情報と認証情報テーブル23の認証情報を対比して機器認証を行う。そして、認証サーバ9は、認証結果をCE機器3に送信する。

10 ステップ6：CE機器3は、認証サーバ9から受信した認証結果をサービスサーバ10に送信し、サービスの提供を要求する。

サービスサーバ10は、認証結果を受信してCE機器3の認証結果を判断し、CE機器3が認証サーバ9により認証された場合はCE機器3にサービスを提供し、認証されていない場合はその旨のアラームをCE機器3に送信し、サービスの提供は行わない。

15 このように、企業情報振り分けサーバ6（第1の振り分けサーバ）と認証先振り分けサーバ8（第2の振り分けサーバ）を合わせて、CE機器3に振り分け先の接続情報を送信する振り分けシステムとして見ることができる。そして、この振り分けシステムは、サービスサーバ10から振り分け情報（機器ID13、企業情報15）を受信する振り分け情報受信手段と、認証サーバ9への接続情報（URL）を送信する接続情報送信手段を備えている。

また、この振り分けシステムの機能を企業情報振り分けサーバ6と認証先振り分けサーバ8の機能を併せ持つ一台の振り分けサーバで実現することもできる。

25 更に、このように、企業情報振り分けサーバ6と認証先振り分けサーバ8を振り分けシステムと見た場合、サービスサーバ10は、CE機器

3 から振り分け情報を受信する振り分け情報受信手段と、振り分けシステムに振り分け情報を送信する振り分け情報送信手段と、振り分けシステムから認証サーバ 9 への接続情報を受信する接続情報受信手段と、受信した接続情報を C E 機器 3 に送信する接続情報送信手段を備えている。

5 また、振り分けシステムを構成する個々のサーバを見た場合、企業情報振り分けサーバ 6 (第 1 の振り分けサーバ) は、サービスサーバ 10 から第 1 の振り分け情報 (企業情報 15) を受信してサービスサーバ 10 に認証先振り分けサーバ 8 (第 2 の振り分けサーバ) への接続情報を送信し、認証先振り分けサーバ 8 は、サービスサーバ 10 から第 2 の振り分け情報 (機器 ID 13) を受信して、認証サーバ 9 への接続情報を送信している。

第 7 図は、第 2 の実施形態における機器認証システム 1 でサービスサーバ 10 が C E 機器 3 に認証を要するサービスを提供する手順を説明するためのフローチャートである。

15 また、サービスサーバ 10 、企業情報振り分けサーバ 6 、認証先振り分けサーバ 8 は、フローチャート中に四角で囲ったような各手順を備えている。

まず、C E 機器 3 がサービスサーバ 10 に認証を要するサービスの提供を要求する (ステップ 105) 。

20 これに対し、サービスサーバ 10 は、機器認証トリガを C E 機器 3 に送信し、機器 ID 13 のサービスサーバ 10 への送信を要求する (ステップ 130) 。

25 C E 機器 3 は、サービスサーバ 10 から機器認証トリガを受信し、自己の機器 ID 13 を読み出してサービスサーバ 10 に送信する (ステップ 110) 。

サービスサーバ10は、CE機器3から機器ID13を受信する（振り分け情報受信手段）。そして、サービスサーバ10は、この機器ID13から企業情報15を抽出して企業情報振り分けサーバ6に送信する（第1の送信手段）（ステップ135）。

5 これにより、サービスサーバ10は、企業情報振り分けサーバ6に対してCE機器3がどの認証先振り分けサーバ8に接続したらよいかの確認を要求する。

企業情報振り分けサーバ6は、サービスサーバ10から企業情報15を受信し（受信手段）、これをキーとして振り分けサーバテーブル21からCE機器3が接続すべき認証先振り分けサーバ8への接続情報を検索する。そして検索された接続情報をサービスサーバ10に送信する（送信手段）（ステップ160）。

サービスサーバ10は、企業情報振り分けサーバ6から接続情報を受信し（第1の受信手段）、これを用いて認証先振り分けサーバ8に接続する。そして、サービスサーバ10は、認証先振り分けサーバ8に、CE機器3から受信した機器ID13を送信し（第2の送信手段）、CE機器3がどの認証サーバ9に接続したらよいかの確認を要求する（ステップ140）。

これに対し、認証先振り分けサーバ8は、サービスサーバ10から機器ID13を受信し（受信手段）、これをキーとして認証サーバテーブル22からCE機器3が接続すべき認証サーバ9への接続情報を検索する。そして検索された接続情報をサービスサーバ10に送信する（送信手段）（ステップ170）。

次に、サービスサーバ10は、認証先振り分けサーバ8から認証サーバ9への接続情報を受信し（第2の受信手段）、これをCE機器3に送信する（接続情報送信手段）。この際に、サービスサーバ10は、CE

機器 3 に認証サーバ 9 で機器認証を受けるように指示する情報である機器認証トリガも C E 機器 3 に送信する（ステップ 145）。

C E 機器 3 は、サービスサーバ 10 から受信した認証サーバ 9 への接続情報を用いて認証サーバ 9 に接続し、認証サーバ 9 と共に一連の機器 5 認証シーケンスを行う（ステップ 115、ステップ 180）。

この機器認証シーケンスは、例えば、機器 ID 13 やパスフレーズなどの認証情報を認証サーバ 9 に送信し、認証サーバ 9 が認証情報テーブル 23 でこれを確認することにより行う。

また、機器認証に伴うデータの送受信を行う前に、例えば、SSL などの暗号技術を用いて C E 機器 3 と認証サーバ 9 の回線接続のセキュリティを確保するように構成してもよい。

認証サーバ 9 は、C E 機器 3 から受信した認証情報により認証結果を C E 機器 3 に送信する（ステップ 185）。このとき、認証サーバ 9 は、サービスサーバ 10 が、後に C E 機器 3 が確かに認証サーバ 9 で認証されたことを確認するためのワンタイムパスワードを発行し、これも C E 15 機器 3 に送信する。

このワンタイムパスワードを発行することにより、認証サーバ 9 と同様な機能を有する偽造サーバなどのなりすましを防止することができる。

認証サーバ 9 は、発行したワンタイムパスワードと、発行対象である 20 C E 機器 3 の機器 ID 13 を対応付けて記憶しておく。

C E 機器 3 は、認証サーバ 9 から受信した認証結果とワンタイムパスワードをサービスサーバ 10 送信し、サービスの提供を要求する（ステップ 120）。この場合も、SSL などの暗号化技術を用いて回線接続のセキュリティを高めることができる。

25 そして、サービスサーバ 10 は、C E 機器 3 から認証結果、機器 ID 13、及びワンタイムパスワードを受信する。

サービスサーバ10は、受信した機器ID13とワンタイムパスワードを認証サーバ9に送信し、CE機器3から受信した認証結果が確かに認証サーバ9が発行したものであるかの認証の確認を認証サーバ9に要求する（ステップ150）。

5 認証サーバ9は、サービスサーバ10から機器ID13とワンタイムパスワードを受信し、先にステップ185で対応付けていた機器ID13とワンタイムパスワードと照合し、確かに認証サーバ9が行った認証であることを確認する。そして認証確認結果をサービスサーバ10に送信する（ステップ190）。

10 なお、以上のステップ150、及びステップ190でのサービスサーバ10と認証サーバ9との通信は、SSLなどの暗号化技術を用いてセキュリティを高めることができる。

15 サービスサーバ10は、認証サーバ9から認証確認結果を受信し、CE機器3から送信されてきた認証結果が確かに認証サーバ9が発行したものであることを確認し、更に、CE機器3から受信した認証結果がCE機器3の認証を証明するものであった場合に、CE機器3に対するサービスの提供を開始する（ステップ155）。

CE機器3は、サービスサーバ10からコンテンツなどのサービス対象を受信し、ユーザがこれを利用する（ステップ125）。

20 なお、ステップ155において、認証サーバ9からの認証の確認が取れなかった場合、あるいは、CE機器3から受信した認証結果が、CE機器3の認証を認めないものであった場合、サービスサーバ10は、CE機器3に対してサービスの提供を行わない。

以上に説明した第2の実施形態では、第1の実施形態で記載した（1）～（4）と同様の効果を得ることができる。

この他に以下のような効果を得ることができる。

(1) 機器認証を要するサービスをサービスサーバ10に要求する場合、CE機器3は、サービスサーバ10に機器ID13を送信し、サービスサーバ10から認証サーバ9への接続情報を受信する。CE機器3が行うこの動作は従来の機器認証システムと同様であるので、CE機器3として従来品を用いることができる。  
5

(2) サービスサーバ10から企業情報振り分けサーバ6へのコンタクトでは、企業情報振り分けサーバ6にパスフレーズや機器ID13を送信する必要が無く、セキュリティを高めることができる。

(3) サービスサーバ10から認証先振り分けサーバ8へのコンタクトでは、認証先振り分けサーバ8にパスフレーズを送信する必要が無く、セキュリティを高めることができる。  
10

## 請求の範囲

1. 端末機器に機器認証を要するサービスを提供する場合に、前記端末機器に第1の振り分けサーバへの接続情報を送信し、前記端末機器から認証結果を受信するサービスサーバと、  
5

端末機器から第1の振り分け情報を受信し、当該第1の振り分け情報に対応する第2の振り分けサーバへの接続情報を送信する第1の振り分けサーバと、

10 端末機器から第2の振り分け情報を受信し、当該第2の振り分け情報に対応する認証サーバへの接続情報を送信する第2の振り分けサーバと、

端末機器から認証情報を受信して機器認証し、認証結果を前記端末機器に送信する認証サーバと、

から構成されたことを特徴とする端末機器認証システム。

2. 請求の範囲第1項に記載の端末機器認証システムでサービスサーバが提供するサービスを利用する端末機器であって、  
15

前記サービスサーバから、第1の振り分けサーバへの接続情報を受信する第1の受信手段と、

前記第1の振り分けサーバに、前記第1の受信手段で受信した接続情報を用いて接続して第1の振り分け情報を送信する第1の送信手段と、

20 前記第1の振り分けサーバから、前記送信した第1の振り分け情報に対応した第2の振り分けサーバへの接続情報を受信する第2の受信手段と、

前記第2の振り分けサーバに、前記第2の受信手段で受信した接続情報を用いて接続して第2の振り分け情報を送信する第2の送信手段と、

25 前記第2の振り分けサーバから、前記送信した第2の振り分け情報に対応した認証サーバへの接続情報を受信する第3の受信手段と、

前記認証サーバに、前記第3の受信手段で受信した接続情報を用いて接続して認証情報を送信する認証情報送信手段と、

前記認証情報送信手段で送信した認証情報による認証結果を前記認証サーバから受信する認証結果受信手段と、

5 前記認証結果受信手段で受信した認証結果を前記サービスサーバに送信する認証結果送信手段と、

を具備したことを特徴とする端末機器。

3. 請求の範囲第1項に記載の端末機器認証システムで端末機器に第2の振り分けサーバへの接続情報を提供する第1の振り分けサーバであって、

端末機器からの接続を受け付け、前記端末機器から第1の振り分け情報を受信する受信手段と、

前記受信した第1の振り分け情報を対応する第2の振り分けサーバへの接続情報を前記端末機器に送信する送信手段と、

15 を具備したことを特徴とする第1の振り分けサーバ。

4. 端末機器に機器認証を要するサービスを提供する場合に、前記端末機器から振り分け情報を受信し、前記受信した振り分け情報を用いて振り分けシステムから認証サーバへの接続情報を受信し、前記受信した接続情報を前記端末機器に送信し、前記認証サーバでの認証結果を前記端末機器から受信するサービスサーバと、

前記サービスサーバから前記振り分け情報を受信し、前記受信した振り分け情報を対応する認証サーバへの接続情報を前記サービスサーバに送信する前記振り分けシステムと、

25 前記端末機器から認証情報を受信して前記端末機器の機器認証を行い、前記機器認証の認証結果を前記端末機器に送信する前記認証サーバと、

から構成されたことを特徴とする端末機器認証システム。

5. 請求の範囲第4項に記載の端末機器認証システムでサービスサーバに認証サーバへの接続情報を提供する振り分けシステムであって、サービスサーバから振り分け情報を受信する振り分け情報受信手段と、前記受信した振り分け情報に対応する認証サーバへの接続情報を送信する接続情報送信手段と、  
5 する接続情報送信手段と、  
を具備したことを特徴とする振り分けシステム。
6. 請求の範囲第4項に記載の端末機器認証システムで端末機器にサービスを提供するサービスサーバであって、端末機器から振り分け情報を受信する振り分け情報受信手段と、  
10 前記受信した振り分け情報を振り分けシステムに送信する振り分け情報送信手段と、  
前記送信した振り分け情報に対応する認証サーバへの接続情報を前記振り分けシステムから受信する接続情報受信手段と、  
前記受信した接続情報を前記端末機器に送信する接続情報送信手段と、  
15 を具備したことを特徴とするサービスサーバ。
7. 前記振り分け情報は、第1の振り分け情報と、第2の振り分け情報から構成され、  
前記振り分けシステムは、  
サービスサーバから前記第1の振り分け情報を受信し、当該第1の振り分け情報に対応する第2の振り分けサーバへの接続情報を前記サービスサーバに送信する第1の振り分けサーバと、  
20 サービスサーバから前記第2の振り分け情報を受信し、当該第2の振り分け情報に対応する認証サーバへの接続情報を前記サービスサーバに送信する第2の振り分けサーバと、  
25 から構成されたことを特徴とする請求の範囲第5項に記載の振り分けシステム。

8. 請求の範囲第7項に記載の振り分けシステムから認証サーバへの接続情報を受信するサービスサーバであって、

　　端末機器から第1の振り分け情報と、第2の振り分け情報を受信する振り分け情報受信手段と、

5　　第1の振り分けサーバに接続し、前記受信した第1の振り分け情報を前記第1の振り分けサーバに送信する第1の送信手段と、

　　前記第1の振り分けサーバから、前記送信した第1の振り分け情報に対応する前記第2の振り分けサーバへの接続情報を受信する第1の受信手段と、

10　　前記第2の振り分けサーバに、前記第1の受信手段で受信した接続情報を用いて接続して前記第2の振り分け情報を送信する第2の送信手段と、

　　前記第2の振り分けサーバから、前記送信した第2の振り分け情報に対応する前記認証サーバへの接続情報を受信する第2の受信手段と、

15　　前記第2の受信手段で受信した接続情報を前記端末機器に送信する接続情報送信手段と、

　　を具備したことを特徴とするサービスサーバ。

9. 請求の範囲第7項に記載の振り分けシステムでサービスサーバに第2の振り分けサーバへの接続情報を提供する第1の振り分けサーバであって、

　　サービスサーバから第1の振り分け情報を受信する受信手段と、

　　前記受信した第1の振り分け情報に対応する第2の振り分けサーバへの接続情報を送信する送信手段と、

　　を具備したことを特徴とする第1の振り分けサーバ。

25　　10. 請求の範囲第7項に記載の振り分けシステムでサービスサーバに認証サーバへの接続情報を提供する第2の振り分けサーバであって、

サービスサーバから第2の振り分け情報を受信する受信手段と、  
前記受信した第2の振り分け情報に対応する認証サーバへの接続情報を  
を送信する送信手段と、  
を具備したことを特徴とする第2の振り分けサーバ。

5 11. 請求の範囲第1項に記載の端末機器認証システムでサービスサ  
ーバが提供するサービスをコンピュータで利用する端末機器方法であつ  
て、  
前記コンピュータは、第1の受信手段と、第1の送信手段と、第2の  
受信手段と、第2の送信手段と、第3の受信手段と、認証情報送信手段  
10 と、認証結果受信手段と、認証結果送信手段と、を具備し、  
前記サービスサーバから、第1の振り分けサーバへの接続情報を前記  
第1の受信手段で受信する第1の受信ステップと、  
前記第1の振り分けサーバに、前記第1の受信ステップで受信した接  
続情報を用いて接続して第1の振り分け情報を前記第1の送信手段で送  
15 信する第1の送信ステップと、  
前記第1の振り分けサーバから、前記送信した第1の振り分け情報に  
対応した第2の振り分けサーバへの接続情報を前記第2の受信手段で受  
信する第2の受信ステップと、  
前記第2の振り分けサーバに、前記第2の受信ステップで受信した接  
続情報を用いて接続して第2の振り分け情報を前記第2の送信手段で送  
20 信する第2の送信ステップと、  
前記第2の振り分けサーバから、前記送信した第2の振り分け情報に  
対応した認証サーバへの接続情報を前記第3の受信手段で受信する第3  
の受信ステップと、

前記認証サーバに、前記第3の受信ステップで受信した接続情報を用いて接続して認証情報を前記認証情報送信手段で送信する認証情報送信ステップと、

前記認証情報送信ステップで送信した認証情報による認証結果を前記  
5 認証結果受信手段で前記認証サーバから受信する認証結果受信ステップ  
と、

前記認証結果受信ステップで受信した認証結果を前記サービスサーバ  
に前記認証結果送信手段で送信する認証結果送信ステップと、

から構成されたことを特徴とする端末機器方法。

10 12. 請求の範囲第1項に記載の端末機器認証システムで端末機器に  
第2の振り分けサーバへの接続情報を提供する第1の振り分け方法であ  
って、

受信手段と、送信手段を備えたコンピュータにおいて、

前記受信手段で、端末機器からの接続を受け付け、前記端末機器から  
15 第1の振り分け情報を受信する受信ステップと、

前記送信手段で、前記受信した第1の振り分け情報に対応する第2の  
振り分けサーバへの接続情報を前記端末機器に送信する送信ステップと、  
から構成されたことを特徴とする第1の振り分け方法。

13. 請求の範囲第4項に記載の端末機器認証システムでサービスサ  
ーバに認証サーバへの接続情報を提供する振り分け方法であって、

振り分け情報受信手段と、接続情報送信手段と、を備えたコンピュー  
タシステムにおいて、

前記振り分け情報受信手段で、サービスサーバから振り分け情報を受  
信する振り分け情報受信ステップと、

25 前記接続情報送信手段で、前記受信した振り分け情報に対応する認証  
サーバへの接続情報を送信する接続情報送信ステップと、

から構成されたことを特徴とする振り分け方法。

14. 請求の範囲第4項に記載の端末機器認証システムで端末機器にサービスを提供するサービス提供方法であって、

5 振り分け情報受信手段と、振り分け情報送信手段と、接続情報受信手段と、接続情報送信手段と、を備えたコンピュータにおいて、

前記振り分け情報受信手段で、端末機器から振り分け情報を受信する振り分け情報受信ステップと、

前記振り分け情報送信手段で、前記受信した振り分け情報を振り分けシステムに送信する振り分け情報送信ステップと、

10 前記接続情報受信手段で、前記送信した振り分け情報に対応する認証サーバへの接続情報を前記振り分けシステムから受信する接続情報受信ステップと、

前記接続情報送信手段で、前記受信した接続情報を前記端末機器に送信する接続情報送信ステップと、

15 から構成されたことを特徴とするサービス提供方法。

15. 請求の範囲第7項に記載の振り分けシステムから認証サーバへの接続情報を受信するサービスサーバ方法であって、

20 振り分け情報受信手段と、第1の送信手段と、第1の受信手段と、第2の送信手段と、第2の受信手段と、接続情報送信手段と、を備えたコンピュータにおいて、

前記振り分け情報受信手段で、端末機器から第1の振り分け情報と、第2の振り分け情報を受信する振り分け情報受信ステップと、

第1の振り分けサーバに接続し、前記受信した第1の振り分け情報を前記第1の送信手段で前記第1の振り分けサーバに送信する第1の送信ステップと、

前記第1の振り分けサーバから、前記送信した第1の振り分け情報に  
対応する前記第2の振り分けサーバへの接続情報を前記第1の受信手段  
で受信する第1の受信ステップと、

前記第2の振り分けサーバに、前記第1の受信ステップで受信した接  
5 続情報を用いて接続して前記第2の振り分け情報を、前記第2の送信手  
段で送信する第2の送信ステップと、

前記第2の振り分けサーバから、前記送信した第2の振り分け情報に  
対応する前記認証サーバへの接続情報を前記第2の受信手段で受信する  
第2の受信ステップと、

10 前記第2の受信手段で受信した接続情報を前記接続情報送信手段で前  
記端末機器に送信する接続情報送信ステップと、

をから構成されたことを特徴とするサービスサーバ方法。

16. 請求の範囲第7項に記載の振り分けシステムでサービスサーバ  
に第2の振り分けサーバへの接続情報を提供する第1の振り分け方法で  
15 あって、

受信手段と、送信手段と、を備えたコンピュータにおいて、

サービスサーバから第1の振り分け情報を前記受信手段で受信する受  
信ステップと、

前記受信した第1の振り分け情報に対応する第2の振り分けサーバへ  
20 の接続情報を前記送信手段で送信する送信ステップと、

から構成されたことを特徴とする第1の振り分け方法。

17. 請求の範囲第7項に記載の振り分けシステムでサービスサーバ  
に認証サーバへの接続情報を提供する第2の振り分け方法であって、

受信手段と、送信手段と、を備えたコンピュータにおいて、

25 サービスサーバから第2の振り分け情報を前記受信手段で受信する受  
信ステップと、

前記受信した第2の振り分け情報に対応する認証サーバへの接続情報を前記送信手段で送信する送信ステップと、  
から構成されたことを特徴とする第2の振り分け方法。

18. 請求の範囲第1項に記載の端末機器認証システムでサービスサーバが提供するサービスを利用するコンピュータで構成された端末機器において、

前記サービスサーバから、第1の振り分けサーバへの接続情報を受信する第1の受信機能と、

10 前記第1の振り分けサーバに、前記第1の受信機能で受信した接続情報を用いて接続して第1の振り分け情報を送信する第1の送信機能と、

前記第1の振り分けサーバから、前記送信した第1の振り分け情報に対応した第2の振り分けサーバへの接続情報を受信する第2の受信機能と、

15 前記第2の振り分けサーバに、前記第2の受信機能で受信した接続情報を用いて接続して第2の振り分け情報を送信する第1の送信機能と、

前記第2の振り分けサーバから、前記送信した第2の振り分け情報に対応した認証サーバへの接続情報を受信する第3の受信機能と、

前記認証サーバに、前記第3の受信機能で受信した接続情報を用いて接続して認証情報を送信する認証情報送信機能と、

20 前記認証情報送信機能で送信した認証情報による認証結果を前記認証サーバから受信する認証結果受信機能と、

前記認証結果受信機能で受信した認証結果を前記サービスサーバに送信する認証結果送信機能と、

を実現する端末機器プログラム。

19. 請求の範囲第1項に記載の端末機器認証システムで端末機器に第2の振り分けサーバへの接続情報を提供するコンピュータで構成された第1の振り分けサーバにおいて、

5 端末機器からの接続を受け付け、前記端末機器から第1の振り分け情報5を受信する受信機能と、

前記受信した第1の振り分け情報を対応する第2の振り分けサーバへの接続情報を前記端末機器に送信する送信機能と、

を実現する第1の振り分けプログラム。

20. 請求の範囲第4項に記載の端末機器認証システムでサービスサーバに認証サーバへの接続情報を提供するコンピュータから構成された振り分けシステムにおいて、

サービスサーバから振り分け情報を受信する振り分け情報受信機能と、

前記受信した振り分け情報を対応する認証サーバへの接続情報を送信する接続情報送信機能と、

15 を実現する振り分けプログラム。

21. 請求の範囲第4項に記載の端末機器認証システムで端末機器にサービスを提供するコンピュータで構成されたサービスサーバにおいて、

端末機器から振り分け情報を受信する振り分け情報受信機能と、

前記受信した振り分け情報を振り分けシステムに送信する振り分け情報送信機能と、

前記送信した振り分け情報を対応する認証サーバへの接続情報を前記振り分けシステムから受信する接続情報受信機能と、

前記受信した接続情報を前記端末機器に送信する接続情報送信機能と、を実現するサービスサーバプログラム。

22. 請求の範囲第7項に記載の振り分けシステムから認証サーバへの接続情報を受信するコンピュータで構成されたサービスサーバにおいて、

5 端末機器から第1の振り分け情報と、第2の振り分け情報を受信する振り分け情報受信機能と、

第1の振り分けサーバに接続し、前記受信した第1の振り分け情報を前記第1の振り分けサーバに送信する第1の送信機能と、

10 前記第1の振り分けサーバから、前記送信した第1の振り分け情報に 対応する前記第2の振り分けサーバへの接続情報を受信する第1の受信機能と、

前記第2の振り分けサーバに、前記第1の受信機能で受信した接続情報を用いて接続して前記第2の振り分け情報を送信する第2の送信機能と、

15 前記第2の振り分けサーバから、前記送信した第2の振り分け情報に 対応する前記認証サーバへの接続情報を受信する第2の受信機能と、

前記第2の受信機能で受信した接続情報を前記端末機器に送信する接続情報送信機能と、

を実現するサービスサーバプログラム。

23. 請求の範囲第7項に記載の振り分けシステムでサービスサーバに第2の振り分けサーバへの接続情報を提供するコンピュータで構成された第1の振り分けサーバにおいて、

サービスサーバから第1の振り分け情報を受信する受信機能と、

前記受信した第1の振り分け情報に対応する第2の振り分けサーバへの接続情報を送信する送信機能と、

25 を実現する第1の振り分けプログラム。

24. 請求の範囲第7項に記載の振り分けシステムでサービスサーバに認証サーバへの接続情報を提供するコンピュータで構成された第2の振り分けサーバにおいて、

サービスサーバから第2の振り分け情報を受信する受信機能と、

5 前記受信した第2の振り分け情報に対応する認証サーバへの接続情報を送信する送信機能と、  
を実現する第2の振り分けプログラム。

25. 請求の範囲第18項に記載の端末機器プログラムを記憶したコンピュータが読み取り可能な記憶媒体。

10 26. 請求の範囲第19項に記載の第1の振り分けプログラムを記憶したコンピュータが読み取り可能な記憶媒体。

27. 請求の範囲第20項に記載の振り分けプログラムを記憶したコンピュータが読み取り可能な記憶媒体。

15 28. 請求の範囲第21項、又は22項に記載のサービスサーバプログラムを記憶したコンピュータが読み取り可能な記憶媒体。

29. 請求の範囲第23項に記載の第1の振り分けプログラムを記憶したコンピュータが読み取り可能な記憶媒体。

30. 請求の範囲第24項に記載の第2の振り分けプログラムを記憶したコンピュータが読み取り可能な記憶媒体。

20 31. 前記第3の受信手段で受信した認証サーバへの接続情報を記憶する接続情報記憶手段と、

前記サービスサーバから前記第1の振り分けサーバへの接続情報を受信した場合に前記接続情報記憶手段で前記接続情報を記憶しているか否かを確認する確認手段と、

25 を具備し、

前記確認手段で前記接続情報が記憶されていることが確認された場合、前記認証情報送信手段は、前記記憶されている接続情報を用いて前記認証サーバに接続して認証情報を送信することを特徴とする請求の範囲第2項に記載の端末機器。

5 3 2. 前記認証情報送信手段は、前記接続情報記憶手段で記憶している前記接続情報を用いて前記認証サーバに接続できなかった場合、前記第1の受信手段で受信した接続情報を元に、前記第1の送信手段、前記第2の受信手段、前記第2の送信手段、及び前記第3の受信手段を用いて取得される認証サーバの接続情報を用いて前記認証サーバに接続して  
10 認証情報を送信し、

前記接続情報記憶手段は、前記取得した認証サーバへの接続情報を用いて、記憶してある接続情報を更新することを特徴とする請求の範囲第31項に記載の端末機器。

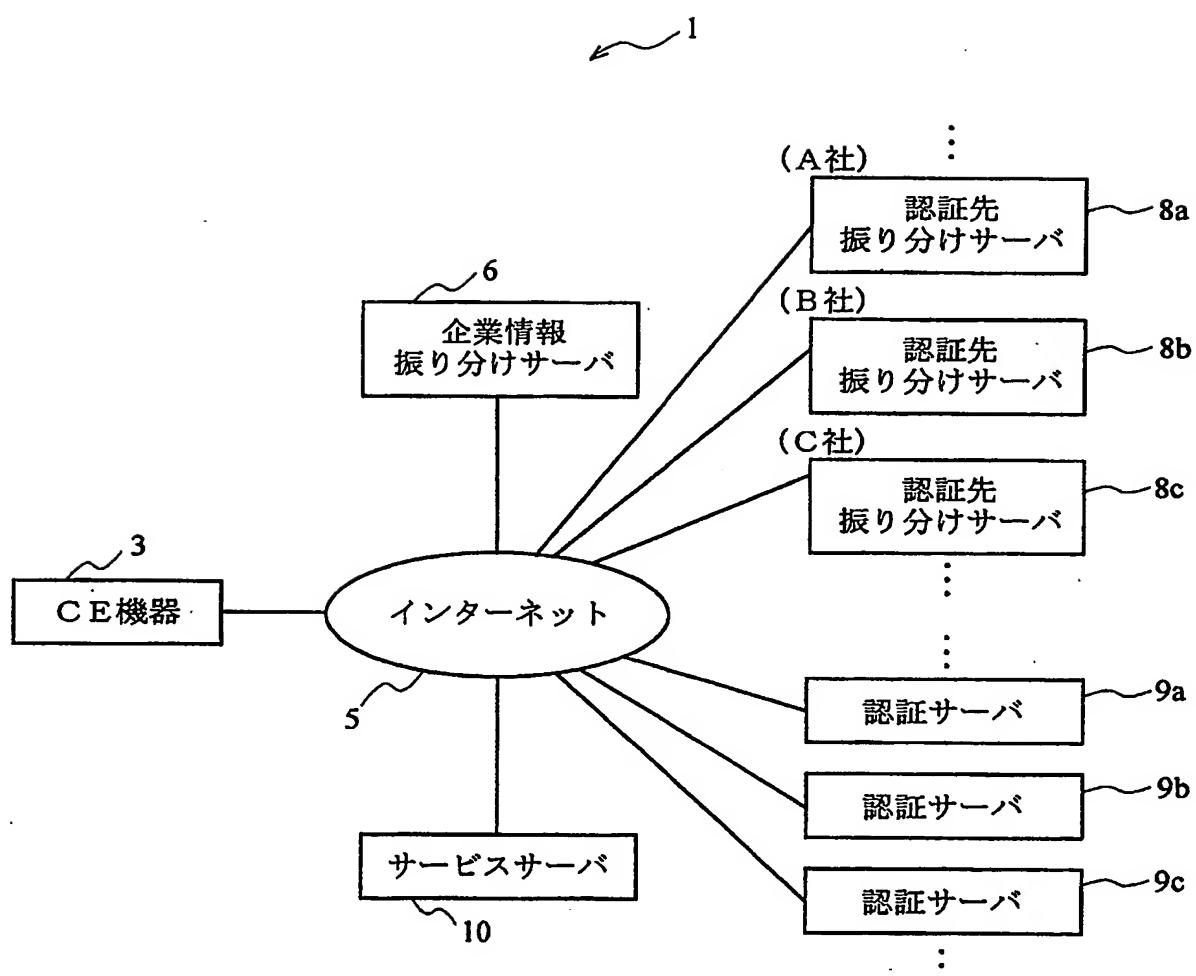


Fig.1

2/8

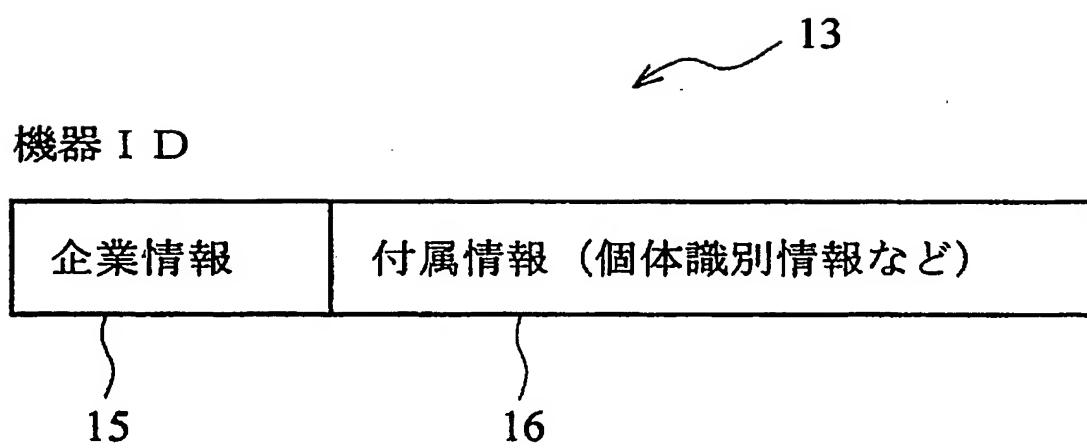


Fig.2

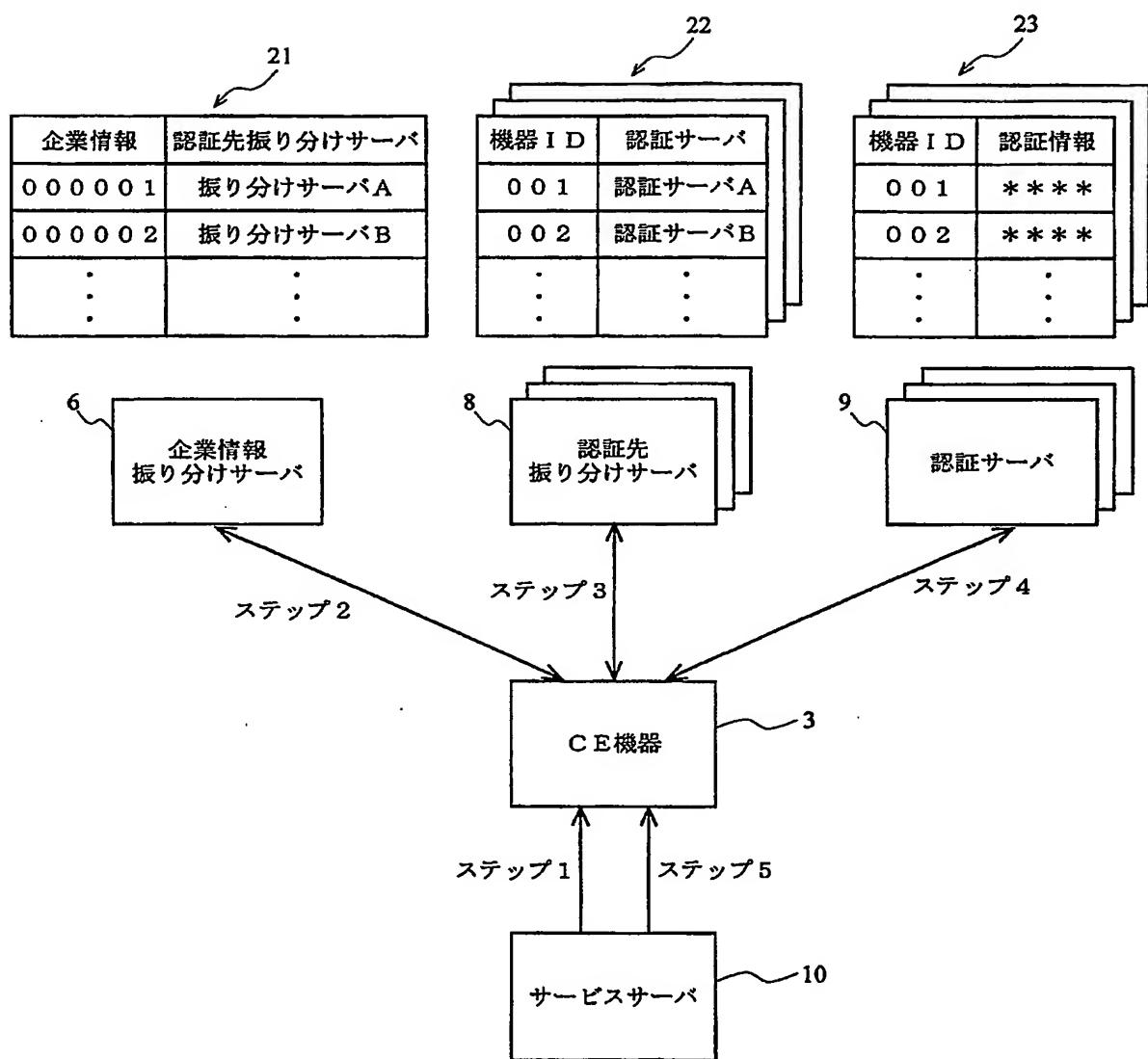


Fig.3

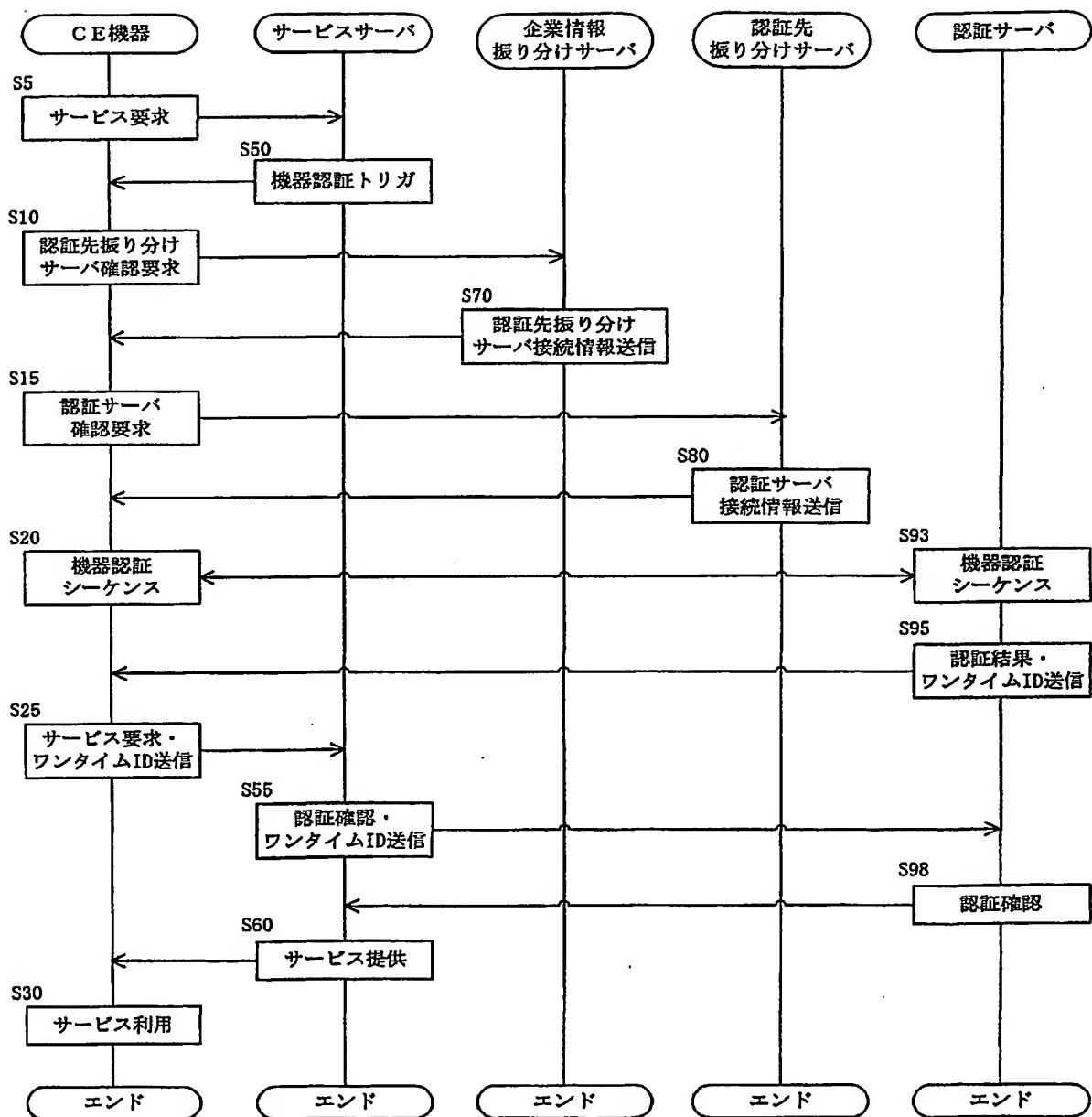


Fig.4

```

<embed with=0 height=0 hidden=true
type="application/x-zony-device-authenticate"
src=http://servicesite.com/dummy.sda
inquireServiceURL="https://oidispatch1.uncuor.zony.co.jp/soap/rpcrouter
inquireService="urn:xxxx:xxxx:soap-object-name#getDA ServerDispInfo"
targetURL="https://servicesite.com/Target.jsp" 33
errorURL=http://servicesite.com/Error.jsp 32
requestVersion="2.1.1,3.1.1" 34
</embed> 35

```

Fig.5A

```

41 <embed with=0 height=0 hidden=true
      type="application/x-zony-device-authenticate"src=http://servicesite.com/dummy.sda>
<X-device-authenticate>
  <inquireServiceURL>https://oidispatch1nd.uncuor.zony.co.jp/soap/rpcrouter</inquireServiceURL>
  <inquireService>urn:xxxx:xxxx:soap-object-name#getDA ServerDispInfo</inquireService>
  <targetURL>http://xxxxxx</targetURL> 44
  <errorURL>http://xxxxxx</errorURL> 45
  <requestVersion>2.1.1,3.1.1</requestVersion> 46
</X-device-authenticate>
50 <X-device-authenticate>
  <inquireServiceURL>https://oidispatch2nd.uncuor.sony.co.jp/soap/rpcrouter</inquireServiceURL>
  <inquireService>urn:xxxx:xxxx:soap-object-name#getDA ServerDispInfo</inquireService>
  <targetURL>http://xxxxxx</targetURL>
  <errorURL>http://xxxxxx</errorURL>
  <requestVersion>2.1.1,3.1.1</requestVersion>
</X-device-authenticate>
</embed>

```

Fig.5B

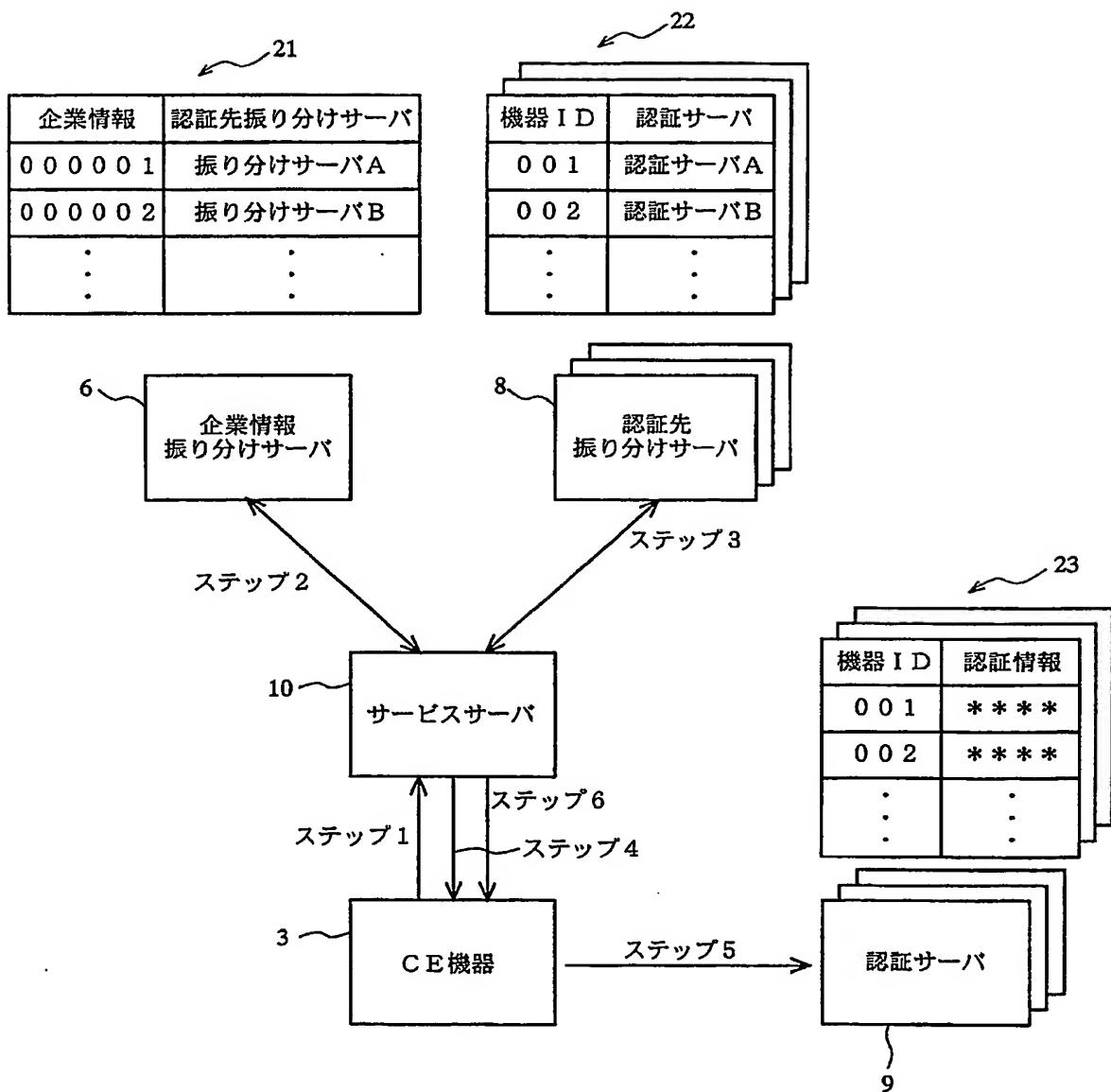


Fig.6

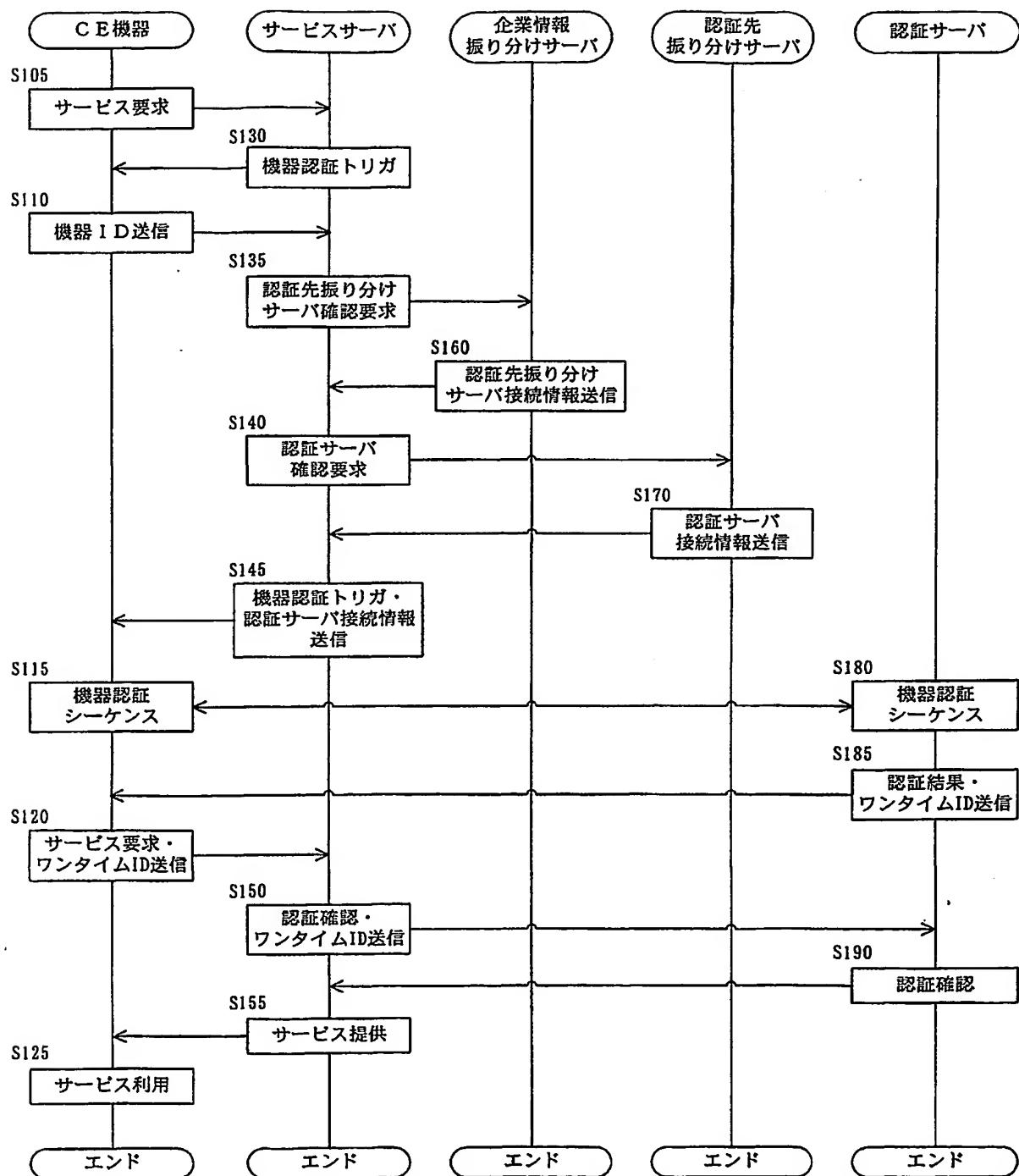


Fig.7

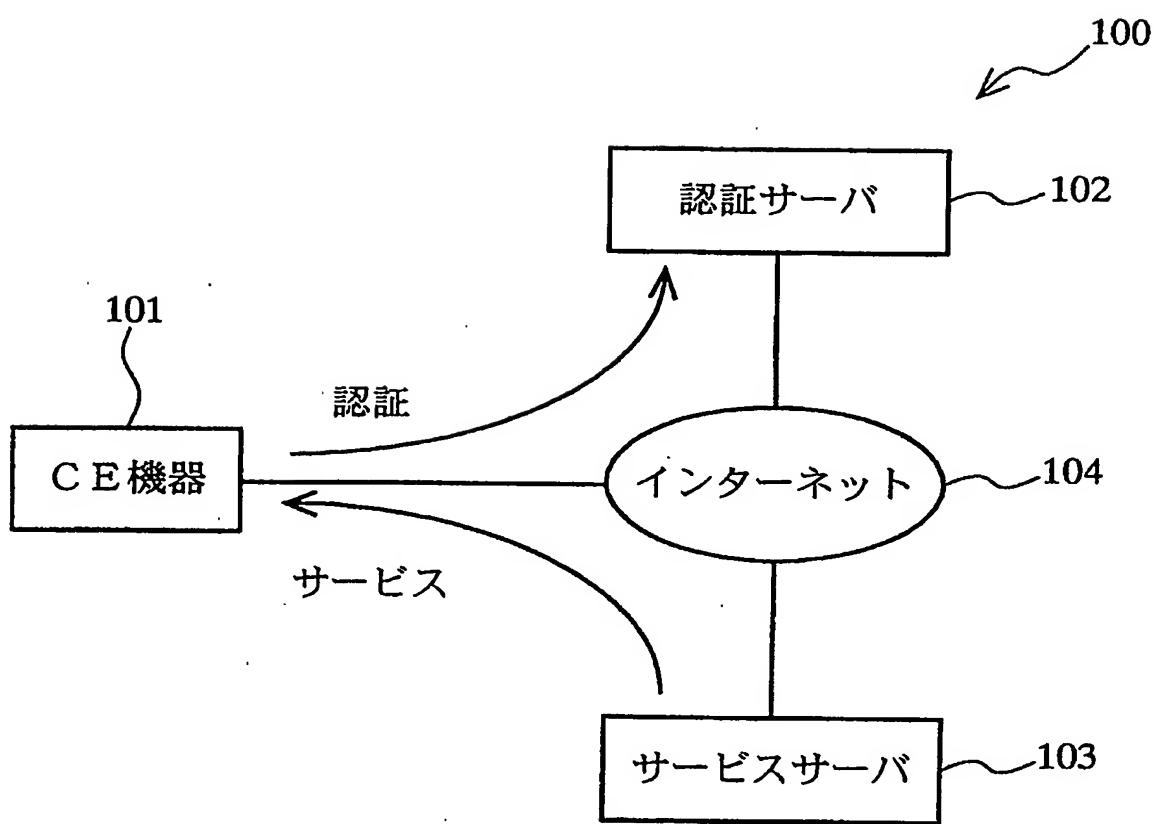


Fig.8

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/JP2004/005740

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl' G06F15/00, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl' G06F15/00, H04L9/32, G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2004  
Kokai Jitsuyo Shinan Koho 1971-2004 Toroku Jitsuyo Shinan Koho 1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-207649 A (NEC Corp. et al.), 26 July, 2002 (26.07.02), Claims (Family: none)	1-32
A	JP 2002-73556 A (Nippon Telegraph And Telephone Corp.), 12 March, 2002 (12.03.02), Claims (Family: none)	1-32
A	JP 2002-82911 A (NEC Corp.), 22 March, 2002 (22.03.02), Claims; Fig. 3 & EP 1186984 A2 & US 2002/38422 A1	1-32

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:	
"A" document defining the general state of the art which is not considered to be of particular relevance	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	"&" document member of the same patent family

Date of the actual completion of the international search 03 August, 2004 (03.08.04)	Date of mailing of the international search report 17 August, 2004 (17.08.04)
---	--

Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No. PCT/JP2004/005740
--

**C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-259606 A (International Business Machines Corp.), 13 September, 2002 (13.09.02), Claim 1 & US 2002/120579 A1	1-32

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl' G06F15/00, H04L9/32

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl' G06F15/00, H04L9/32, G06F17/60

## 最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国実用新案登録公報	1996-2004年
日本国登録実用新案公報	1994-2004年

## 国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2002-207649 A (日本電気株式会社他) 2002.07.26 特許請求の範囲 (ファミリーなし)	1-32
A	JP 2002-73556 A (日本電信電話株式会社) 2002.03.12 特許請求の範囲 (ファミリーなし)	1-32
A	JP 2002-82911 A (日本電気株式会社) 2002.03.22 特許請求の範囲及び図3 & EP 1186984 A2 & US 2002/38422 A1	1-32

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」同一パテントファミリー文献

## 国際調査を完了した日

03.08.2004

## 国際調査報告の発送日

17.8.2004

## 国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許序審査官 (権限のある職員).

宮司 阜佳

5B 9555

電話番号 03-3581-1101 内線 3545

C (続き) 関連すると認められる文献		関連する 請求の範囲の番号
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	
A	JP 2002-259606 A(インターナショナル・ビジネス・マシーンズ・ コーポレーション) 2002.09.13, 請求項 1 & US 2002/120579 A1	1-32